fairtrials.org

Law and Policy on the use of Artificial Intelligence by Police and Criminal Justice Systems

November 2024

Fairness, equality, justice

Fair Trials is an NGO that campaigns for fair and equal criminal justice systems. Our team of independent experts expose threats to justice through original research and identify practical changes to fix them. We campaign to change laws, support strategic litigation, reform policy and develop international standards and best practice.

We do this by supporting local movements for reform and building partnerships with lawyers, activists, academics, and other NGOs. We are the only NGO that campaigns exclusively on the right to a fair trial, giving us a comparative perspective on how to tackle failings within criminal justice systems globally.

We coordinate the Legal Experts Advisory Panel (LEAP) – the leading criminal justice network in Europe consisting of over 180 criminal defence law firms, academic institutions and civil society organisations. More information about this network and its work on the right to a fair trial in Europe can be found here.

OPEN SOCIETY
FOUNDATIONS

This report was made possible thanks to the support of Open Society Foundations (OSF).

@fairtrials @fairtrials Fair Trials

First published by Fair Trials in November 2024. © Fair Trials 2024.

Graphic design: Anne-Cécile Fraud https://annececile.myportfolio.com/

Table of Contents

1. Introduction

Currently, artificial intelligence (AI) is revolutionizing various sectors, including the functioning of police and criminal justice systems. However, this technology poses significant risks, especially in terms of privacy, fair trial, equality, and non-discrimination. Globally, various countries are beginning to develop regulatory frameworks to address these risks and ensure that the use of AI aligns with human rights and fundamental freedoms.

This study aims to identify the current state of play in the context of the regulation and policies surrounding the use of AI by security authorities and the criminal justice system in Europe. Through a comprehensive analysis, we will explore how different countries have approached the regulation of AI, identifying common themes and specific regulatory measures implemented. The report will focus on legal and policy frameworks, providing examples to illustrate how these regulations are applied in practice.

2. Methodology

a. Concept of Artificial Intelligence

Artificial intelligence, as a field of study, encompasses automated and algorithmic decision- making and big data. Despite no agreed-upon definition of artificial intelligence, it is possible to say that it is a field that can be broken down into systems that think and act like humans[1]. Under that framework, automated and algorithmic decision-making and big data are part of artificial intelligence. In addition, AI works through algorithms, although not all algorithms include AI. In this document we will use the concept of AI, although we recognize there are different levels of automatization applied to systems used by police and criminal justice authorities.

b. Legal and theoretical analysis

While NGOs have documented the negative consequences of the misuse of artificial intelligence, this report will focus solely on how governments regulate technology that incorporates AI, not on its application.
Fair Trials previously documented the impacts of artificial intelligence on human rights, with notable findings included in the Fair Trials report Automating Injustice[2]. One issue identified in that report is the lack of regulation about the use of AI by law enforcement and criminal justice authorities. For that reason, we considered it necessary to develop a report that identified the state of play of regulation and policies related to the use of artificial intelligence by authorities responsible for

[1] Access Now, human rights in the age of artificial intelligence, p. 8.

[2] Fair Trials, Automating Injustice: The use of artificial intelligence & automated decision-making systems in criminal justice in Europe. (9 September 2021) https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf.

security and the criminal justice system. This is not a report on the application of artificial intelligence tools. Nor does the report analyze the effectiveness of the available legal mechanisms, although in some cases examples are provided to better illustrate the existing regulation or policy.

c. Human rights framework

We have chosen the human rights framework to systematize the regulation on the use of artificial intelligence by security authorities and the criminal justice system. Relevant human rights are privacy, fair trial, equality, and non-discrimination.

d. Caveats

Below are various caveats that should be considered to clarify the scope of the report.

i. Varied AI applications across countries

Countries covered in the report apply AI to police and criminal justice authorities in different ways. This clarification will help better understand why certain countries have fewer regulations than others.

ii. Scope of findings

Some aspects of the findings are outside the scope of this investigation. For example, AI can be used for public health systems or education processes (e.g. in Spain).

iii. Different legal traditions

Legal regulations come from different traditions. While common law applies in the UK, civil law applies in Spain, Germany, and France. The UK, for example, has an uncodified constitution, whereas countries like Germany, which are also federal states, have more specific constitutional and legal regulations. Additionally, most countries have unitary governments, but Germany has a federal government. This is relevant because, for example, there are local regulations with many specificities in Germany.

iv. Exclusion of application issues

The analysis will include issues regarding the application of AI laws, despite the report's aim not to review effectiveness of regulation. Examples of the application of laws will help to improve understanding of the content of certain regulations.

3. Overview of the use of artificial intelligence

The most widely used artificial intelligence-based tool by security forces in Europe is facial recognition. At this point, it is important to clarify that not all surveillance camera equipment has the capability to perform facial recognition, meaning it does not have artificial intelligence- based capabilities.

Likewise, some countries have used predictive tools in criminal investigations. Below is a brief overview of each technology.

The **Belgian** police tried to use automated facial recognition surveillance systems during a testing phase at the Brussels Airport. These surveillance systems were subsequently banned[3] as the Police Services Act (which generally allows for the use of intelligent cameras[4]) does not allow for the creation of a database that would facilitate comparing camera images with the existing biometric data of individuals.

Belgian police forces are seeking to implement a nationwide predictive policing system (called "iPolice") which is a collaborative effort between the Ministry of Home Affairs, the Digital Agenda, and the Ministry of Justice. This initiative aims to centralize all police data on the cloud.[5]The new system is expected to enter into operation before the end of 2025 and is expected to cost approximately EUR 300 million.[6]The system aims to automatically search other relevant official databases, such as the national register or judicial databases. Algorithms will be used to compare the available data with images from surveillance cameras, photos, fingerprints and other stored documents.[7]

In the meantime, local police forces have already been working on their own implementation of predictive policing systems, such as the local Westkust police zone (including municipalities of Koksijde, De Panne and Nieuwpoort)[8] and the local Zennevallei police zone (including the municipalities of Beersel, Halle, and Sint-Pieters-Leeuw).[9]

[3] Bert Peeters, "Facial recognition at Brussels Airport: face down in the mud", KU Leven, (17 March 2020), https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in-the-mud/.

[4] Ibid.

[5] Algorithm Watch, Automating Society Report 2020, https://algorithmwatch.org/en/automating-society/#:~:text=The%202020%20edition,lens%20on%20the%20EU%20level.

[6] Andreas Kockartz, "'i-Police, die digitale Revolution' der belgischen Polizei (8 May 222), https://www.vrt.be/vrtnws/de/2022/05/08/i-police-die-digitale-revolution-der-belgischen-polizei-wi/.

[7] Ibid.

[8] Haco, "Politiezone Westkust experimenteert met datasets in strijd tegen criminaliteit" (17 May 2016), https://www.standaard.be/cnt/dmf20160517_02292901.

[9] European Digital Rights, Use cases: "Impermissible AI and fundamental rights breaches" (August 2020).

In **France**, the Internal Security Code ISC also includes specific provisions relating to the Rapid Automated Border Crossing system (known as "PARAFE"),[10] which enables the use of a facial recognition system to improve and facilitate police controls at external borders for air, sea and rail passengers.[11]

Also in **France**, the laws governing the Olympic Games ('Olympic Games Law') allow for algorithmic processing of images collected by means of video-protection systems and airborne cameras to detect and report certain events. This measure aims to ensure the security of the Olympic Games and other events. This is a significant departure for the French system.

In **France**, the Criminal Procedure Code (CPC) includes provisions relating to databases used by enforcement authorities, including:

- **TAJ** ("Traitement des antécédents judiciaires" or Prior Criminal History database).[12]This enables the police to perform automated processing of personal data collected during investigations into serious criminal areas to facilitate the detection of certain criminal offenses, as well as the gathering of evidence and search for perpetrators.

- **Automated national judicial database** of perpetrators of sexual or violent offenses ("**FIJAISV**"), used to prevent reoffending and to facilitate the identification of perpetrators.[13]

- **Serial assessment databases** which enable national police to carry out automated processing on data collected during certain investigations and procedures, to gather evidence and identify perpetrators through establishing links between individuals, events or serial criminal offenses.[14]

- **Automated fingerprint database** ("**FAED**") is used to search for and identify the perpetrators of crimes and misdemeanors, as well as persons sentenced to deprivation of liberty. It also facilitates the search for missing persons and the identification of the deceased or seriously injured. It is also used to verify the identity of detainees.[15]

- **Automated DNA database** ("**FNAEG**") is used to facilitate the identification and search for offenders using their genetic profile, and for missing persons using the genetic profile of their descendants or relatives.[16]

- **Automated national judicial database of perpetrators** of terrorist offenses ("**FIJAIT**").[17]

- **Wanted persons database** ("**FPR**") lists all persons subject to a search, or

[10] 'Passage Automatisé Rapide Aux Frontières extérieures'.

[11] Articles R. 232-6 et seq. ISC.

[12] Articles 230-6 et seq.of the French Criminal Procedure Code.

[13] Articles 706-53-1 et seq. of the French Criminal Procedure Code.

[14] Article 230-12 of the French Criminal Procedure Code.

[15] Article R40-38-1 of the French Criminal Procedure Code.

[16] Articles 706-54 à 706-56-1-1 of the French Criminal Procedure Code.

[17] Articles 706-25-3 to 706-25-14 CPC.

verification of legal status, to facilitate searches carried out by police at the request of judicial, military, or administrative authorities.[18]

In **Germany** processing personal data by the police has been regulated by police laws of most of the German states. Taking the example of Baden-Württemberg, the most relevant regulations under this police law (PolG-BW[19]) are the following:

- The police have the authority to make visual and audio recordings of persons for the purpose of identifying and averting danger. The police may also automatically evaluate the recordings made beforehand. Consequently, this provision allows for the use of "smart" CCTV cameras to detect patterns of behaviour.[20]
- The police have the authority to request the transmission of data of certain persons from public and non-public bodies to carry out an automated comparison with other databases. Such data transfer requires the order of a court.[21]
- The police are authorized to use automatic license plate reading systems. The license plate numbers recorded can be automatically compared with the police information system maintained by the Federal Criminal Police Office.[22]

The following additional provision is noteworthy:

- Under Section 59 of the Saxon law on police enforcement (Sächsisches Polizeigesetz - "SächsPVDG"[23]), police enforcement has been authorized to use automatic facial recognition on public roads in border areas in order to combat cross-border crime.

In **Poland**, limited information is available regarding the current utilization of new technologies by law enforcement authorities. Reports indicate the use of automated case allocation systems, AI tools for prison surveillance, and electronic decision-making to enhance judicial efficiency. However, specific operational details about these systems remain limited.

In **Spain**, the Spanish Ministry of Interior intends to use and is already experimenting with the algorithm "*ABIS*" which is expected to be used to identify suspects from a database of filed photographs. The algorithm will show a percentage determining whether the features of the face in the image more or less match those stored in the database. If the algorithm reveals a 100% match between the suspect in question and the photographs on file, it is likely that the relevant person has been identified.

[18] Article 230-19 CPC.

[19] Police law Baden Württemberg, 6 October 2020, https://www.landesrecht- bw.de/jportal/?quelle=jlink&query=PolG+BW&psml=bsbawueprod.psml&max=true&aiz=true.

[20] Section 44 PolG-BW.

[21] Section 48 PolG-BW.

[22] Section 51 PolG-BW.

[23] Saxon law on police enforcement services, 11 May 2019, https://www.revosax.sachsen.de/vorschrift/18193-Saechsisches-Polizeivollzugsdienstgesetz-.

The **UK** uses Live Facial Recognition (LFR) primarily for law enforcement purposes. The College of Policing has issued guidance for deploying LFR, emphasizing its responsible and transparent use. The technology is used to locate individuals on watchlists and is integrated with big-data ecosystems to prevent crime and anti-social behaviour.

4. Legal regulation

In most of the analyzed countries, there is no specific regulation on the use of artificial intelligence in the criminal justice system. However, existing regulation allows for the limitation of use.

The human rights legal framework serves as a legal basis to limit the use of AI-based technologies. In this regard, the European Convention on Human Rights complements national constitutions and other domestic legal instruments. Additionally, every country of the European Union has implemented the common European regulation in its domestic law.

In this section, we will first refer to the common regulation on personal data protection and then review the specific regulations applicable in certain countries.

a. Human Rights

i. European Convention on Human Rights (ECHR)

All the countries analyzed are States Parties to the European Convention on Human Rights (ECHR). However, certain particularities must be considered. For example, in the UK the Human Rights Act 1998 also exists, which strengthens certain rights and freedoms guaranteed in the ECHR.[24]

Additionally, several countries have ratified treaties from the universal human rights system, such as the International Covenant on Civil and Political Rights (ICCPR).

ii. International, constitutional, and domestic regulation

Every country guarantees a series of rights under its constitution. These are reviewed below based on four rights: fair trials, privacy, data protection and equality, and non-discrimination.

The Right to a Fair Trial

The right to a fair trial is explicitly stated in Article 6(1) ECHR and Article 47 Charter

[24] Human Rights Act 1998 chapter 42 available at https://www.legislation.gov.uk/ukpga/1998/42/introduction.

of Fundamental Rights of the European Union.[25]

In **Belgium**, Article 23 of the constitution states the right to lead a life worthy of human dignity such as the right to legal assistance.

In **France**, Article 6 of the European Convention on Human Rights is a key provision, ensuring "*everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal*". While the Constitution and the (Declaration of the Rights of Man and of the Citizen of 1789) DRHC do not expressly refer to the right to a fair trial, the Constitutional Council held that the right to a fair trial is protected by Article 16 of the DRHC.[26]

In **Germany**, the right to a fair trial is one of the essential principles of a procedure based on constitutional rules. It is not explicitly mentioned in the Basic Law, but its roots can be seen in Article 20(3) of the Constitution (GG) in conjunction with Article 2(1) GG.[27]Article 20(3) of the Basic Law binds the legislature to the constitutional order and the executive power and the judiciary to law and justice. Furthermore, the free development of the personality of every human being is guaranteed by Article 2(1) GG.

The right to a fair trial is expressed in other laws, such as the Criminal Procedure Code (e.g., mandatory defence in some criminal procedures[28] or the prohibition of surprising decisions in civil procedures[29] according to the Code of Civil Procedure (Zivilprozessordnung – "ZPO"[30])).

In **Poland**, Article 45 (1) establishes that everyone shall have the right to a fair and public hearing of his case, without undue delay, before a competent, impartial, and independent court.

In **Spain**, Article 24[31] of the Constitution sets out the right to a fair trial, ensuring ' All persons have the right to obtain effective protection from the judges and the courts in the exercise of their rights and legitimate interests, and in no case may there be a lack of defence…' as well as ' …all have the right to the ordinary judge predetermined by law; to defence and assistance by a lawyer; to be informed of the charges brought against them; to a public trial without undue delays and with full guarantees; to the use of evidence appropriate to their defence; not to

[25] Charter of fundamental rights of the European Union, 18 December 2000, https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[26] Constitutional Council, Decision No. 2004-510 DC of 20 January 2005.

[27] Bundesverfassungsgericht (Federal Constitutional Court), `Decision of April 21, 2016, 2BvR 1422/15, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rk20160421_2b vr142215.html.

[28] Section 140 StPO.

[29] Section 139 (2) ZPO.

[30] Code of Civil Procedure, 10 October 2013, https://www.gesetze-im- internet.de/englisch_zpo/englisch_zpo.html.

[31] Article 24, Spanish Constitution, 29 December 1978.

make self-incriminating statements; not to plead themselves guilty; and to be presumed innocent.'

In the **UK**, a country with an uncodified constitution, the Human Rights Act 1998 provides for the right to a fair and public trial or hearing within a reasonable time by an independent and impartial tribunal established by law.

Privacy

The general right to privacy is enshrined in Article 22 of the **Belgian** Constitution, specifying that Belgians have the right to the respect of their private and family life, except in the cases and conditions determined by law.

In **France**, the constitution and the DRHC do not expressly protect the right to a private life (hereafter, the "right to privacy"). However, the Constitutional Council held that the right to privacy can be derived from Article 66 of the Constitution as well as Article 2 of the DRHC, which protects individuals' "*natural and imprescriptible rights*".[32]

In addition to the constitution and the DRHC, other domestic provisions protect the right to privacy, including Article 9 of the Civil Code, which provides that "*everyone has the right to respect for their private life*", and Articles 226-1 et seq. of the Criminal Code, which provides for criminal fines and prison sentences for certain privacy breaches.

In **Germany**, the right to privacy is known as the right to informational self-determination and derives from the general right of personality and human dignity pursuant to Articles 2(1) GG and 1(1) GG. The right to privacy is also specified in Article 12 of the Universal Declaration of Human Rights, in Article 8(1) ECHR, and in Article 7 of the Charter of Fundamental Rights of the European Union.

In **Poland**, Article 47 of the Constitutional Privacy Regulation states ' Everyone shall have the right to legal protection of his private and family life.'

In **Spain,** Article 18[33] of the constitution includes three fundamental rights of privacy: the right to honour, privacy, and personal image. These rights are inalienable and inherent to the individual and cannot be waived. They are also personal and non-transferable.

In the **UK,** Article 8 of the Human Rights Act protects an individual's right to respect for private and family life.

Data protection

This right will be reviewed in the section below regarding protection laws.

[32] Constitutional Council, Decisions No. 94-352 of 18 January 1995 and no. 99-416 of 23 July 1999.

[33] Article 18, Spanish Constitution, 29 December 1978.

Equality and non-discrimination

The right of equality without discrimination is guaranteed by Articles 10 and 11 of the **Belgian** Constitution.

Article 1 of the constitution provides that **France** shall ensure the equality of all citizens before the law, without distinction of origin, race, or religion, and shall respect all beliefs. Article 6 of the DRHC provides that the law must be the same for all, whether it protects or punishes. In addition, other specific provisions prohibit discrimination. For instance, Article 95 prohibits profiling that discriminates against individuals on the basis of sensitive data, in the context of processing operations for a law enforcement purpose.

The key equality provision in the **Polish** Constitution is Article 32(1) 'All persons shall be equal before the law. All persons shall have the right to equal treatment by public authorities' and Article 32(2) 'No one shall be discriminated against in political, social or economic life for any reason whatsoever'.

In **Spain** Article 14[34] of the Constitution provides that 'Spaniards are equal before the law, without any discrimination based on birth, race, sex, religion, opinion or any other personal or social condition or circumstance.'

In the **UK** Article 14 of the Human Rights Act protects the enjoyment of the rights and freedoms in the ECHR without discrimination on the grounds of 'sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status'. 'Other status' includes sexual orientation, illegitimacy, marital status, trade union membership, transsexual status and imprisonment, family status[35], age, or disability based on case law. Case law states that freedom from discrimination also covers 'indirect discrimination'.

b. Common regulation in Europe

i. The General Data Protection Regulation (GDPR)

The GDPR is a European Union Regulation that governs data protection. The GDPR is applicable, as of 25 May 2018, in all member states of the European Union, including Belgium, France, Germany, Poland and Spain, to harmonize data privacy laws. The Data Protection Act 2018, which implemented GDPR in the UK remains in force.

It sets out mandatory rules for how organizations and companies may process personal data. However, according to Article 2(2)(d) GDPR, the Regulation does not apply where personal data is processed by competent police or law enforcement authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, including

[34] Spanish Constitution, 29 December 1978.

[35] R (L and others) v Manchester City Council.

the safeguarding against and the prevention of threats to public security.[36]

ii. Law Enforcement Data Protection Directive (EU) 2016/680 (LED)

The Law Enforcement Directive (LED) is applicable in Belgium, France, Germany, Poland and the UK. It protects citizens' fundamental rights to data protection whenever personal data is used by criminal law enforcement authorities for law enforcement purposes.[37]

The LED specifically regulates the law enforcement authorities' processing of personal data and requires competent authorities to prevent, investigate, detect or prosecute criminal offences and execute criminal penalties, including safeguarding against and preventing threats to public security.[38]This is the key difference with respect to the GDPR which does not apply to the processing of personal data for law enforcement purposes.

Each EU member state has implemented the LED in different ways. For example, Belgium applies data protection rules to processing operations by authorities, including intelligence services, for the safeguarding of national security. This is because member states are allowed to provide for higher standards of protection beyond the LED and, as such, may extend its applicability to processing activities in pursuit of national security.[39]

The directive requires that the personal data collected by law enforcement authorities is processed lawfully and fairly, collected for specified, explicit and legitimate purposes, appropriately secured and not kept for any longer than is necessary, among other requirements.[40]However, the Belgian implementing legislation merely states that the logs used for criminal proceedings may only be used for the general purposes of the LED. A study prepared by the Directorate-General for Internal Policies on the 'Assessment of the implementation of the Law Enforcement Directive' concluded that this provision may be interpreted in an overly broad fashion, leading to unintended use of the logs for various police operations and as evidence in general criminal proceedings, rather than just those involving system use and data access.[41]

The data subjects under the LED are those who have been convicted of a criminal

[36] Regulation (EU) 2016/679, Article 2(2)(d).

[37] The Data Protection Law Enforcement Directive, Data Protection in the EU, European Commission, https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#:~:text=The%20Data%20Protection%20Law%20Enforcement%20Directive,-Directive%20(EU)%202016&text=The%20directive%20protects%20citizens'%20fundamental,authorities%20for%20law%20enforcement%20purposes.

[38] Directive (EU) 2016/680, Article 1.

[39] Policy Department for Citizens' Rights and Constitutional Affairs, "Assessment of the Implementation of the Law Enforcement Directive" (December 2022).

[40] Directive (EU) 2016/680, Article 4.

[41] Policy Department for Citizens' Rights and Constitutional Affairs, "Assessment of the Implementation of the Law Enforcement Directive" (December 2022).

offence (which serves as serious grounds for believing that they have committed or are about to commit a criminal offence), victims (or potential victims) of a criminal offence, as well as other parties such as those who may be called to testify.[42]

iii. Artificial Intelligence Act (2021/0106(COD) («EU AI Act»)

In April 2021, the European Commission proposed the Artificial Intelligence Act[43] in the form of a regulation. Regulation is binding throughout every EU member state after its date of application, including Belgium, France, Germany, Poland and Spain.

The proposed Artificial Intelligence Act had the following objectives:

- ensure that AI systems used in the EU are safe and respect existing laws, fundamental rights and EU values;
- enhance governance and effective enforcement of existing laws, fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

In September 2022 the European Commission proposed a directive on adapting non- contractual civil liability rules to artificial intelligence, the AI Liability Directive[44]. The directive aims to make it easier for victims to claim compensation for damages caused by AI systems. Victims do not have to prove the causal link between the fault and the output of the AI system. Rather, the directive creates a rebuttable presumption. Under the directive, national courts have the power to order disclosure of evidence about high-risk AI systems which are suspected to have caused damages.
In June 2023 the EU Parliament adopted amendments to the proposal for the EU AI Act.

Belgium has, however, previously maintained[45] that policymakers must always be alive to the reality that AI systems can be easily repurposed for a variety of uses. As a result, there must be a balance between specialization and consistency for certain sectors (e.g. law enforcement). In relation to the use of such systems for predictive policing, Belgium previously intimated that clarity is key particularly to how such legislation would work in practice. This would ensure that concrete defined exceptions exist to guarantee that such rules can be employed in a

[42] Data Protection Act 2018, Article 31.

[43] EUR-Lex, `Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI-Act) and amending certain union legislative acts`, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

[44] EUR-Lex, `Proposal for a Directive of the European Parliament and of the Council on adapting non- contractual civil liability rules to artificial intelligence`, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496.

[45] Council of the European Union, Artificial Intelligence Act – BE comments Article 1-29, Annexes I-IV (3 November 2021).

workable and effective manner.

The Scientific Service of the German Parliament states that there are "no current legislative processes for the enactment of corresponding (artificial intelligence) regulations"[46] in Germany.

Spain held the presidency of the Council of the EU for the last six months of 2023. During this period, it was tasked with fostering dialogue regarding the development of AI regulation to address the ethical, legal and societal ramifications of AI. The draft EU AI Act was predicated on the principles of transparency and accountability. The Act requires AI-based systems to be transparent in their functioning so that users can understand how decisions are taken, and the logic behind them. Articles 13, 14 and 15 of the Act mandate that high-risk AI systems should be designed and developed in such a way that their operation is sufficiently transparent so that users can interpret the system's output and use it appropriately. Additionally, the articles require that there are appropriate human-machine interface tools to enable oversight, and that users are informed that they are interacting with an AI system.[47]

The EU AI Act also sets forth in Article 17[48] that use of high-risk AI systems by developers, service providers and businesses, will require compliance with regulations which mandate testing, proper documentation of data quality, and an accountability framework that details human oversight of the relevant AI system.

Article 9 of the EU AI Act, by virtue of the 'Risk Management System'[49] prohibits intrusive and discriminatory uses of AI, such as predictive policing systems and remote biometric identification.

The European Parliament adopted the final version of the EU Artificial Intelligence Act on 13 March 2024[50]. The EU published Regulation 2024/1689 of the EU Artificial Intelligence Act on 12 July 2024[51].

Other positive developments include the establishment of the European Commission's AI Office (The European AI Office) on 24 January 2024[52]. It will monitor, supervise and enforce the AI Act requirements on general purpose AI

[46] Scientific Service of the German Parliament, `Regulation of artificial intelligence in Germany with special regard to the health care sector`, 2023, https://www.bundestag.de/resource/blob/937082/7dd12737cdf4123fdf35d06cb56bcb24/WD-9-002-23-pdf-data.pdf.

[47] 'Key Issues: Transparency Obligations', EU AI Act https://www.euaiact.com/key-issue/5.

[48] Article 17, Quality Management System, EU AI Act https://www.euaiact.com/article/17.

[49] Article 19, Risk Management System, EU AI Act https://www.euaiact.com/article/9.

[50] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

[51] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689.

[52] Commission Decision Establishing the European AI Office, https://digital- strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office.

(GPAI) models and systems across the 27 EU member states.[53]

c. Artificial Intelligence-related laws

Specific regulations of each country related to artificial intelligence used by criminal justice and police authorities will be reviewed.

i. Belgium

The **Belgian** Constitution provides victims with the right to file a complaint with the Constitutional Court if their rights have been violated.

ii. France

In France, the Internal Security Code created in 2012 ("ISC")[54]governs the use of video protection systems and mobile cameras by public authorities, including the police, military, military police (*gendarmerie*) and customs. The ISC governs the use of airborne cameras.[55] This includes cameras installed on unmanned aircraft, such as drones, tethered balloons, airplanes, and helicopters.

In January 2021 the French Data Protection Authority (CNIL) ordered the Interior Ministry to comply with data protection laws and to cease collection of personal data through drones equipped with cameras by police forces, until a legal or regulatory framework authorising such data processing was put in place[56].

The Criminal Code provides for criminal fines and prison sentences, for certain discriminatory actions.[57]The right to equality and the prohibition of discrimination could provide protection for individuals in cases where big data, AI or other technologies were being used by enforcement authorities to target specific groups.

CNIL and France's Defender of Rights expressed concerns about the impact of algorithms on fundamental rights. CNIL notably raised the risks of bias when commenting on the Draft Bill for Biometric Recognition.

In May 2020 the Defender of Rights, jointly with CNIL published a report entitled "*Algorithms: preventing automated discriminations*" in which they recommended increased support for research to develop methodologies to reduce and prevent bias, strengthened information and transparency obligations and the training of professionals. They also recommended that impact studies be conducted to

[53] The AI Office: What is it, and how does it work?, https://artificialintelligenceact.eu/the-ai-office-summary/.

[54] Internal Security Code (available at: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000025503132/).

[55] Articles L. 242-1 et seq. and Articles R. 242-1 et seq. of the ISC.

[56] CNIL, Deliberation SAN-2021-003 of 12 January 2021.

[57] Articles 225-1 et seq. of the French Criminal Code.

anticipate the discriminatory effects of algorithms.[58]

Over the past few years, France has adopted several laws amending the ISC, aimed at further regulating video protection systems and mobile cameras and their use by public authorities. While these laws enable enforcement authorities to use video protection systems and mobile cameras, they continue to prohibit the use of facial recognition. Even the controversial 'Olympic Games Law', which allows the automated processing of data collected by video protection systems and mobile cameras, prohibits facial recognition and the processing of biometric data.

The French Parliament debated the use of biometric and facial recognition technologies by public authorities. On 12 June 2023, the Senate adopted a Draft Bill on Biometric Recognition in the Public Space, which contemplates authorizing the use of these technologies in exceptional cases.

In addition, the ISC also states that on-board cameras cannot be equipped with automated facial recognition. The Constitutional Court clarified that these provisions cannot be interpreted as authorizing authorities to analyze images using other automated facial recognition systems not directly installed on cameras.[59] On-board cameras cannot automatically link, align or combine this data with other personal data sets.

The ISC, as recently amended by the Criminal Liability and Internal Security Law of 24 January 2022,[60] provides that the administrative authority may implement video monitoring in police custody and customs detention cells to prevent the risk of escape and threats to the person placed under police custody.[61]

Placement under video monitoring is subject to certain conditions which include restrictions on the length of monitoring and the requirement to obtain the authorization of the judicial authority for monitoring beyond 24 hours. Video surveillance cannot be coupled with any biometric or sound recording device and there should be no automated alignment, combination or linkage with other personal data sets.

PARAFE

The ISC also includes specific provisions relating to the Rapid Automated Border Crossing system (known as "PARAFE"),[62] which enables the use of facial recognition to improve police controls at external borders for air, sea and rail passengers.[63]

[58] Defender of Rights (May 2020), *Algorithms: preventing automated discriminations* (available at: https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/synth-algos-en-num-16.07.20.pdf).

[59] Constitutional Council, Decision no. 2021-834 DC of January 20, 2022.

[60] Criminal Liability and Internal Security Law (available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045067923).

[61] Article L. 256-1 of the ISC.

[62] 'Passage Automatisé Rapide Aux Frontières extérieures'.

[63] Articles R. 232-6 et seq. ISC.

The PARAFE system consists of automated control gates located at certain border checkpoints. The individual enters a booth where the system compares the image on the individual's passport or travel document with the live photo of the individual taken inside the booth. If both photos match, the individual can then exit the booth and cross the gate.

The system is based on the consent of individuals, who can choose to go through the system or opt for a traditional booth with a border guard.

'Olympic Games Law'[64]

Article 10 of the 'Olympic Games Law' provides that images collected by means of video- protection systems and airborne cameras may be subject to algorithmic processing to detect and report certain events. This measure aims to ensure the security of the Olympic Games and other events.

The use of these technologies under the 'Olympic Games Law' is an experiment, which will last until 31 March 2025 and will be subject to an evaluation report at the end of 2024[65]. There is little doubt that if the reports' findings are positive, the Government and Parliament will consider a more lasting use of this technology.

Article 10 of the law provides for several guarantees and limitations, notably:

- This technology can only be used during specific events, including the Olympic and Paralympic Games as well as other sporting, recreational or cultural events, which, due to the scale of the attendance or their circumstances, are particularly exposed to the risk of acts of terrorism or serious threats to people's safety.
- The sole purpose of the algorithmic data processing is to detect, in real time, predetermined events likely to present or reveal risks (e.g. crowd movements, packages, suspicious behavior in venues hosting events and on public transport), and to report them to enable the national and municipal police, the national police, fire and rescue services and the SNCF's and RATP's security services to implement any necessary preventative measures.
- The public must be informed in advance, and by appropriate means, of the use of algorithmic processing of images collected by video protection systems and airborne cameras, unless circumstances prohibit the transmission of such information or where such information would jeopardize the objective pursued.
- Automated processing operations cannot use any biometric identification system, process any biometric data or use any facial recognition. This assessment is however disputed by several organizations that consider that the relevant technology does indeed process data that amounts to biometric data, since the systems are identifying events or recognizing individuals,

[64] Olympic Games Law (available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047561974).

[65] It will last until 31 March 2025, although the Olympic and Paralympic games will end in September 2024.

based on the behaviour of the individuals filmed.[66]

- Automated processing operations cannot be aligned, combined or automatically linked with other personal data sets.

- Algorithmic processing must incorporate human control measures and a risk management system to prevent and correct the occurrence of any bias or misuse.

- A state representative of the local 'Department' or the 'Préfet de Police' in Paris must authorize the use of the algorithmic processing of images collected by video protection systems and airborne cameras. The authorization, which may only be granted where the processing is proportionate to the objective pursued, must specify its scope and duration.

Despite these guarantees, these provisions were highly controversial and widely disputed by members of the public, organizations such as Amnesty International and political parties.

Some Members of Parliament filed an appeal before the Constitutional Council challenging the validity of various provisions of the 'Olympic Games Law', including Article 10.

In their appeal, the Members of Parliament notably argued that Article 10 infringed the freedom of movement, the right to protest, the freedom of opinion and the right to private life. In this regard, they claimed that guarantees in the law were not sufficient. Furthermore, they argued that the provisions were too wide in scope and that the detection of certain events would necessarily lead to the processing of biometric data, which is technically prohibited. They also argued that Article 10 infringes the principle of equality before the law, since the criteria on which algorithmic processing will be based did not exclude all discrimination.

The Constitutional Council eventually dismissed these arguments. It held that, to meet the constitutional objective of the prevention of breaches of public order, the parliament may authorize the algorithmic processing of images collected by means of video protection systems or airborne cameras, provided that appropriate safeguards to protect the right to private life accompany these systems.[67]

The Constitutional Council considered that the safeguards provided for by the 'Olympic Games Law' were sufficient and that Article 10 did not infringe the right to private life, subject, however, to one reservation. It held that Article 10 should be construed as requiring the state representative who authorized the measure

[66] LQDN's report (available at: https://www.laquadrature.net/wp-content/uploads/sites/8/2023/02/Dossier-VSA-2-LQDN.pdf) Contributions by LQDN and CCLA, LRC, ICCL, Agora, EIPR, ECNL, Privacy International (available at: https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2023850dc/2023850dc_contributions.pdf) and Op-ed by 11 organisations (https://www.lemonde.fr/idees/article/2023/03/06/les-mesures-de-videosurveillance-algorithmique-introduites-par-la-loi-jo-2024-sont-contraires-au-droit-international_6164276_3232.html).

[67] Constitutional Council, Decision No. 2023-850 DC of 17 May 2023.

to immediately revoke the authorization if the conditions which justified its issuance are no longer met.

Draft Bill on Biometric Recognition of 12 June 2023

On 10 May 2022, the Senate's Law Commission adopted a Report entitled *"Biometric recognition in public spaces: 30 proposals to prevent the risk of a surveillance society"*.[68] Following this report, the Senate adopted a Draft Bill on biometric recognition in public.

The draft bill has two main objectives, which are: (i) responding to a need for regulation of biometric systems by creating a specific legal framework and (ii) enabling public authorities to use biometric technologies in exceptional cases. It goes further than the 'Olympic Game Law' as it allows for facial recognition in certain cases.

The draft bill sets out 'red lines', with a general prohibition on the categorization and rating of individuals based on their biometric data. Furthermore, it sets out a general prohibition of the processing of biometric data for the purpose of identifying an individual remotely in public spaces, except where individuals gave their consent.

The draft bill provides for exceptions in certain cases, for instance, allowing the experimental use of biometric processing for major events particularly exposed to the risk of acts of terrorism or serious threats to people's safety, for certain judicial and intelligence investigations or for the fight against terrorism and serious crime. These provisions are subject to strict conditions and safeguards.

On 23 May 2023 the Senate heard CNIL's assessment of the draft bill, which identified five main risks:

- a threat to privacy, since these systems make it possible to identify any person in a photograph or video, undermining as a result the principle of anonymity in public.
- a risk of errors regarding the identification of individuals, as seen in certain countries which initiated use of these systems.
- a risk of discriminatory bias, depending on how the systems have been set up.
- a risk of restriction of rights and fundamental freedoms, e.g. individuals may reconsider attending a demonstration if they know that they will be filmed and potentially recognized.
- a risk of security breaches, especially where biometric databases are centralized.

CNIL stressed that the Parliament had just decided, in the Olympic Games

[68] Senate's Law Commission (10 May 2022), *Biometric recognition in public spaces: 30 proposals to prevent the risk of a surveillance society* (available at: https://www.senat.fr/rap/r21-627/r21-627_mono.html).

Law, to test smart camera technologies, within a very precise and well-defined framework, which did not include facial recognition. They called on the Senate to restrict the scope of the bill and adhere to the balance struck by the 'Olympic Game Law' for the time being.

The Senate adopted the draft bill on 12 June 2023 and sent it to the National Assembly. As explained above, this draft bill was proposed by the party "Les Républicains" and is unlikely to be adopted by the National Assembly, given the current political context and the Government's reservations on the draft.

Law Enforcement Directive

The **Law Enforcement Directive** (LED) was implemented in Title III of the Data Protection Act and Title III of the Decree.

Title III of the Data Protection Act[69] governs the processing of personal data for the purpose of the prevention and detection of criminal offences, investigation and prosecution of criminal offices and/or the execution of criminal sanctions. This includes protection against threats to public security and their prevention (a 'Law Enforcement Purpose'), by any competent public authority or any other body or entity entrusted with the exercise of public authority and of the prerogatives of public authority (a 'Competent Authority').

The processing of personal data for a Law Enforcement Purpose must be authorized by order of the competent Minister adopted after consulting CNIL.[70]

Article 95, which relates to the processing for a Law Enforcement Purpose, provides some safeguards against automated justice and decision-making.

First, Article 95 prohibits profiling that results in discrimination against individuals on the basis of sensitive data.

Second, Article 95 specifies that no judicial decision involving an assessment of a person's behavior may be based on automated processing of personal data intended to evaluate certain aspects of the person's personality.

Some have criticized this provision, pointing out that it only prevents a judge from basing their decisions on profiling algorithms that process personal data. Judges may, however, base their decisions on both profiling algorithms that do not process personal data and algorithms that process personal data but that do not involve profiling.[71]

[69] Title III includes Articles 87 to 114 of the Data Protection Act.

[70] Article 88.

[71] Jean-Baptiste Duclercq (2018), *Les algorithmes en procès*.

Other decisions that have a legal bearing on an individual[72] (e.g. decisions adopted by public administrative authorities), can be based partly on the automated processing of personal data intended to evaluate certain aspects of the individual's personality.

There are no exceptions to this rule. This is in contrast to rules applicable to processing operations carried out for a purpose other than a Law Enforcement Purpose, which set out several exceptions to the general prohibition.[73] Article 47 of the Data Protection Act, which relates to processing operations carried out for a purpose other than a Law Enforcement Purpose, prohibits decisions based solely on automated processing intended to evaluate the individual's personality.

In 2018 the Constitutional Council confirmed the validity of the use of algorithms, as it considered that there were sufficient safeguards, i.e. right to appeal and prohibition to base a decision solely on a profiling algorithm when the processing involve sensitive data.[74]

There are limited publicly reported cases relating to Article 95 of the Data Protection Act. Some cases concern the adoption of decisions by public administrative authorities, based on the presence of individuals in criminal databases. Complaints are generally dismissed where it is demonstrated that the decisions were not adopted solely based on the information included in those databases but also considered the individual's specific situation.

For instance, in several cases, administrative courts dismissed appeals lodged by individuals who had been prohibited from acquiring a weapon and subject to a weapon divestiture procedure, after consultation of the Prior Criminal History database (the "TAJ" *traitement des antécédents judiciaires*) showed that they had previously been convicted of criminal offences (e.g. driving a vehicle under the influence of alcohol, sexual assault).[75]

[72] It covers all decisions producing legal effects, not only decisions producing adverse legal effects as provided for by Article 11 the Law Enforcement Directive.

[73] Article 47 of the Data Protection Act, which relates to processing operations carried out for a purpose other than a Law Enforcement Purpose, also prohibits decisions producing legal effects for or significantly affecting an individual based solely on automated processing intended to evaluate that individual's personality. However, it sets out several exceptions to the prohibition. Notably, individual administrative decisions may be based solely on automated processing, including profiling, where certain conditions are met, namely: (i) the decisions must be adopted in compliance with Article L. 311- 3-1 and Chapter I of Title I of Book IV of the French Code on Relations between the Public and the Administration (relating to the information of the individual concerned and the right to appeal the decision), (ii) the processing cannot concern sensitive data, (iii) the decisions must include an explicit statement informing the interested party of the automated processing, as provided for by Article L. 311- 3-1 of the French Code oN Relations between the Public and the Administration and (iv) the data controller must ensure that the algorithmic processing and its evolution are under control, so as to be able to explain, in detail and in an intelligible form, to the data subjects the way in which the processing has been implemented with regard to them.

[74] Constitutional Council, Decision No. 2018-765 DC of 12 June 2018.

[75] E.g. Douai Administrative Court of Appeal, Decision No. 21DA00960 of 22 February 2022; Lille Administrative Court, Decision No. 2108703, 7 June 2023.

Courts made similar findings, based on Article 47 of the Data Protection Act (which relates to processing operations carried out for a purpose other than a Law Enforcement Purpose). For instance, an individual had challenged an administrative decision, which had rejected his request to renew his resident permit on the ground that he had been convicted of drug trafficking as shown in the Schengen Information System ("**SIS**").[76] To dismiss the appeal, the administrative court held that the decision was not based exclusively on the fact that the individual was registered in the SIS file. The decision was also based on the fact that the individual had been convicted of drug trafficking and therefore constituted a threat to public order.

The Criminal Procedure Code (CPC) includes provisions relating to various databases used by enforcement authorities, including:

- **TAJ** ("*Traitement des antécédents judiciaires*" or Prior Criminal History database).[77] The CPC enables national police to perform automated processing of personal data collected during investigations into certain serious criminal offenses, to enhance detection of criminal offences, gather evidence and search for perpetrators. TAJ refers both to automated processing and the resultant database.

- **automated national judicial database** of perpetrators of sexual or violent offences ('**FIJAISV**') used to prevent reoffending and to facilitate the identification of perpetrators.[78]

- **serial assessment databases** which enable national police in charge of judicial police duties to carry out automated processing of data collected during certain investigations and identify perpetrators by establishing links between individuals, events or criminal offenses.[79]

- **automated fingerprint database** ('**FAED**'), which is used to search for and identify perpetrators of crimes and misdemeanors, as well as persons sentenced to deprivation of liberty. It facilitates the search for missing persons and the identification of the dead, seriously injured and detainees.[80]

- **automated DNA database** ('**FNAEG**') which is used to facilitate the identification and search for offenders using their genetic profile, and for missing persons using the genetic profile of their descendants or ascendants.[81]

- **automated national judicial database of perpetrators** of terrorist offenses ('**FIJAIT**').[82]

- **wanted persons database** ('**FPR**') which lists all persons subject to a search

[76] Nancy Administrative Court of Appeal, Decision no. 20NC02391-20NC02760 of 10 May 2021.

[77] Articles 230-6 et seq.of the French Criminal Procedure Code.

[78] Articles 706-53-1 et seq. of the French Criminal Procedure Code.

[79] Article 230-12 of the French Criminal Procedure Code.

[80] Article R40-38-1 of the French Criminal Procedure Code.

[81] Articles 706-54 à 706-56-1-1 of the French Criminal Procedure Code.

[82] Articles 706-25-3 to 706-25-14 CPC.

or verification of legal status, to facilitate searches carried out by police at the request of judicial, military or administrative authorities;[83]

- **national judicial interception platform** (**'PNIJ'**).[84]

The use of these databases is subject to various safeguards and restrictions. These include authorization to access, types of information to be included on the databases, data retention periods and potential supervision by judicial authorities.

Individuals have rights which vary according to the database. These include right to request access, correction and erasure of their personal data (subject to certain conditions). However, these rights do not exist for all databases (e.g. FAED).

TAJ

TAJ has been particularly scrutinized in recent years, and organizations have criticized its ubiquitous use by enforcement authorities.

TAJ includes a facial recognition tool, which enables enforcement authorities to identify an individual *a posteriori*, by comparing an image that they have (e.g. from a CCTV camera) with images included in TAJ.

TAJ use is subject to specific guarantees and limitations, notably the type of individual authorized to access the database,[85] the purpose for database use[86] and the type of information held.[87]

In addition, individuals have specific rights in relation to TAJ, such as a right to request access, correction or erasure of their personal data. However, individuals do not have the right to object to the processing of their personal data, except victims who can object once the perpetrator has been sentenced.[88]

According to CNIL, TAJ includes information relating to 87 million cases and more than 18.9 million records of individuals suspected to have committed a criminal offence. The use of TAJ facial recognition has increased significantly in recent years. According to reports, it was used 498,871 times by the national police and

[83] Article 230-19 CPC.

[84] Article 230-45 CPC.

[85] E.g. national police and national gendarmerie, customs officers, intelligence services, public prosecutors and investigating judges.

[86] It can notably be used in certain judicial, intelligence and administrative investigations.

[87] The TAJ can contain information on victims and suspects, including photographs with technical features that allow the use of a facial recognition device, as well as other information on the case facts. However, images of public places cannot be included.

[88] Articles 230-8 et 230-9 CPC and R. 40-33 CPC.

approximately 117,000 by the national gendarmerie in 2021.[89]

The massive use of TAJ facial recognition has been disputed by organizations in France, and notably by La Quadrature du Net, an organization promoting and defending fundamental freedoms in the digital world, which filed a complaint before the Conseil d'Etat.

La Quadrature du Net argued that the use of TAJ facial recognition was not necessary and was not subject to appropriate safeguards for data rights under Article 10 of the Law Enforcement Directive and Article 88 DPA. However, the Administrative Supreme Court dismissed the complaint. The Court held that the use of facial recognition was absolutely necessary, given the extremely high number of suspects included in TAJ (several million), which makes it impossible to compare images manually with the same level of reliability. The Court also considered that there were appropriate safeguards, and that the system was not disproportionate.[90]

iii. Germany

In addition to the GDPR and the LED, the Federal Data Protection Act (BDSG) is also applied in Germany. BDSG imposes conditions for processing based on automated decision-making. The provision transposes Article 11 of the Law Enforcement Directive.

Pursuant to Section 54(1) BDSG, a decision based solely on automated decision-making, which produces an adverse legal effect concerning the data subject or significantly affects him or her, shall be permitted only when authorized by law. The law could be either a national law or European Union law.

According to the wording of the provision, the decision must be «solely» automated. Additionally, if an organization and/or a public body takes an active role in the decision-making process, the requirement of "solely" is not met. Automated data processing that is merely intended as the basis for a subsequent active police decision, therefore, remains lawful.[91]

Furthermore, the decision must have an «external effect» for the data subject. Mere internal interim determinations or evaluations by the authority are not covered by the scope of this provision.[92]

State laws

[89] Parliamentary Report No. 627 submitted on 10 May 2022, *"Biometric recognition in public spaces: 30 proposals to avert the risk of a surveillance society"* (available at : https://www.senat.fr/rap/r21-627/r21- 627_mono.html).

[90] Conseil d'Etat, 26 April 2022, Decision No. 442364, *La Quadrature du Net*.

[91] *Mundil,* `BeckOK Datenschutzrecht, BDSG, 43. Edition`, Section 54, para. 3, https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FBeckOKDatenS_45%2FBDSG%2Fcont%2FBECKOKDAT%20ENS.BDSG.P54.glA.htm.

[92] German Parliament, Draft legislation, page 112, https://dserver.bundestag.de/btd/18/113/1811325.pdf.

Processing personal data by the police has been regulated in the police laws of most German states. In Saarland and Hamburg, however, the state legislature preferred to implement these provisions as a separate law. The different laws include provisions on data collection, further processing, data transmission, and data protection control.

Taking the example of Baden-Württemberg, the most relevant regulations under this police law (PolG-BW[93]) are the following:

- The police have, under certain circumstances, the authority to make visual and audio recordings of persons for the purpose of identifying and averting danger. The police may automatically evaluate previously made recordings. Consequently, this provision allows for the use of "smart" CCTV cameras to detect patterns of behaviour. It should be noted that the automatic evaluation may only be used to recognize behaviour patterns that suggest the intent to commit a crime.[94]
- The police have the authority to request the transmission of data of certain persons from public and non-public bodies to conduct an automated comparison with other databases. However, such data transfer requires the order of a court.[95]
- Furthermore, the police are authorized to use automatic license plate reading systems. The license plate numbers recorded can be automatically compared with the police information system maintained by the Federal Criminal Police Office. If this comparison does not result in a match with the database, the data collected must be deleted immediately.[96]

In addition, the following two provisions from federal states are noteworthy:

- Under Section 59 of the Saxon law on police enforcement (Sächsisches Polizeigesetz - "SächsPVDG"[97]), the police enforcement has been authorized to use automatic facial recognition on public roads in border areas in order to combat cross-border crime. The Saxon Ministry of the Interior has now decided that this regulation should not continue beyond the end of December 2023 due to a lack of proportionality. However, conventional video surveillance without automated data comparison pursuant to Section 57 SächsPVDG shall continue to be used.[98]
- The police in North Rhine-Westphalia are authorized to link and automatically evaluate a wide variety of collected data using the Gotham software from the

[93] Police law Baden Württemberg, 6 October 2020, https://www.landesrecht- bw.de/jportal/?quelle=jlink&query=PolG+BW&psml=bsbawueprod.psml&max=true&aiz=true.

[94] Section 44 PolG-BW.

[95] Section 48 PolG-BW.

[96] Section 51 PolG-BW.

[97] Saxon law on police enforcement services, 11 May 2019, https://www.revosax.sachsen.de/vorschrift/18193-Saechsisches-Polizeivollzugsdienstgesetz-.

[98] Lto, `Saxony ends automatic facial recognition` https://www.lto.de/recht/nachrichten/n/sachsen- gesichtserkennung-kriminalitaet-grenze-polizei-straftaten/.

Palantir company. The state legislature has created a legal basis for this in Section 23 VI PolG-NRW, which is similar to the laws in Hesse and Hamburg that have been declared unconstitutional by the Federal Constitutional Court.

iv. Poland

The right to the protection of personal data is guaranteed in Article 51 of the Polish Constitution:

- No one may be obliged, except on the basis of statute, to disclose information concerning his person.
- Public authorities shall not acquire, collect or make accessible information on citizens other than that which is necessary in a democratic state ruled by law.
- Everyone has a right to access official documents and other data related to their person. Limitations upon such rights may be established by statute.
- Everyone has the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means other than that established by statute.[99]

The main criminal justice or policing laws concerning collection and usage of data are found in the Police Services Act.[100] Unlike the DPA, which primarily supplements the GDPR and transposes LED provisions relating to processing of personal data in criminal investigations into national law, the Police Services Act deals with police information management and with establishment of a supervisory body.

Additionally, the Police Services Act also sets up rules for the use of visible camera systems by the police within the scope of their mission. The law explicitly mentions the use of an "intelligent camera" which is defined as *"the camera that also contains components and software, which may or may not be linked to registers or files, which can process the collected images autonomously or not"*.[101]

There are very few regulations concerning automated data collection and evaluation. The regulations that exist mainly relate to automated data collection, automatic number plate recognition[102] and the potential use of intelligent cameras.[103] However, the law sets up the requirements and procedures for the handling of personal data and information in accordance with purposes defined in Article 27 of the DPA (i.e. prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security).[104] This

[99] The Polish Constitution, available at https://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm.

[100] "Wet van 5 augustus 1992 op het politieambt (Wet Politieambt)" (B.S. 22 december 1992), https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1992080552&table_na me=loi.

[101] Wet Politieambt, Article 25/2 § 1 No. 3.

[102] Wet Politieambt, Article 44/2 § 3.

[103] Wet Politieambt , Article 25/3.

[104] Wet Politieambt, Article 44/1 § 1.

also includes the right to handle special categories of personal data pursuant to Article 34 of the DPA,[105] while setting up specific requirements for the handling of biometric, health and genetic data.[106]

In general, the Police Services Act differentiates between data collected for administrative police purposes (such as contact details related to the management of events, disturbances in public, individuals who represent a danger to themselves or others)[107] and for judicial police (such as data related to suspects and convicted persons, unsolved deaths, missing persons, witnesses).[108] For these different types of data, differentiated rules apply (e.g. with regard to storage periods and deletion of old information, as well as competencies of the supervisory authority and other agencies).

As Poland is a member of the European Union, the Polish legislative framework in relation to data protection arises mostly from EU regulations and directives. Data protection is governed primarily by the GDPR which has been implemented into Polish national law by virtue of the Act of 10 May 2018 regarding the Protection of Personal Data.[109]

v. Spain

In Spain, the use of automated decision making ("**ADM**") processes by public authorities is covered under Law 40/2015.[110] This text defines *"automated administrative action"* as "*any act or action entirely performed through electronic means by a public administration body as part of an administrative procedure and with no direct intervention by any employee*". The text states that before any automated administrative action is taken a competent authority must be identified *"to define the specifications, programming, maintenance, supervision and quality control and, if applicable, the audit of the information system and its source code"*. Similarly, a competent authority must be identified which would be responsible in the event of a legal challenge to the automated action.

Additionally, Law 19/2013[111] regulates citizens' access to public information, mandating that public bodies must be proactively transparent and in the majority of cases grant citizens access to any content and documents held by public authorities. In practice public bodies rarely publish detailed information regarding the ADM systems they use.

[105] Such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, Directive (EU) 2016/680, Article 34.

[106] Wet Politieambt, Article 44/1 § 2.

[107] Wet Politieambt, Article, 44/5 § 1.

[108] Wet Politieambt, Article 44/5 § 3.

[109] Ustawa z 10 maja 2018 o ochronie danych osobowych, Accessed September 21, 2023. https://uodo.gov.pl/pl/128/1192.

[110] Law 40/2015, 1 October 2015.

[111] Law 19/2013, 9 December 2013.

The GDPR was implemented by Constitutional Law 3/2018,[112] under the Protection of Personal Data and Guarantee of Digital Rights ("**LOPDGDD**").[113] This law introduced and adapted the GDPR, providing a new set of digital rights, in accordance with the mandate contained in Article 18.4[114] of the Constitution, based on the fundamental right of the individual to the protection of personal data.

In addition, Spain has implemented (albeit somewhat late)[115] the LED through Constitutional Law 7/2021[116] and has stayed relatively true to the text of the directive. Constitutional Law 7/2021 operates in parallel with LOPDGDD to the extent that these laws do not conflict with the objectives of the existing regulations that govern these areas. However, the LED's scope extends to regulation of the processing of personal data by competent authorities. Indeed, the use of personal data in criminal proceedings, is set out in Constitutional Law 7/2021, on the protection of personal data processed for the purpose of prevention, detection, investigation and prosecution of criminal offences and execution of criminal sanctions or criminal penalties.

Under Constitutional Law 7/2021, any Spanish national or citizen and any legal entity with a registered office in Spain must cooperate with the requesting police authority, public prosecutor or criminal court to provide information requested, as long as certain data protection requirements are met. These requirements are that the request is limited and specific (proportionality principle) and that the data subject is informed unless a legal exception applies (transparency principle). There is no clear guidance from the Spanish data protection authority (the "**AEPD**") regarding these principles, and, as such, guidance from the EU Commission on the LED would need to be relied upon in these circumstances.

We have not been able to identify any examples of enforcement action under Constitutional Law 7/2021, or any specific case law relating to the restriction of police or law enforcement use of big data and AI. However, there has been widespread criticism of Spanish police use of an algorithmic profiling system *"VioGén"* which was launched by the Spanish Ministry of Interior and is deployed by the police to help evaluate the risk women face of domestic violence (those who have previously filed a domestic abuse complaint). The algorithm, which uses classical statistical models to perform a risk evaluation (which is used to determine how much help a user will receive)[117], has been criticized for *"lacking*

[112] Constitutional Law 3/2018, 6 December 2018.

[113] Protección de Datos Personales y garantía de los derechos digitales.

[114] Article 18, Spanish Constitution, 29 December 1978.

[115] 'New Constitutional Law 7/2021', Easy Telecom Law Firm, 29 06 2021 https://www.easytelecomlaw.com/nueva-ley-de-proteccion-de-datos-7-2021/.

[116] Constitutional Law 7/2021, 26 May 2021.

[117] Melissa Heikkila, 'AI : Decoded: Spain's flawed domestic abuse algorithm – Ban debate heats up – Holding the police accountable', Politico, 16 March 2022, https://www.politico.eu/newsletter/ai- decoded/spains-flawed-domestic-abuse-algorithm-ban-debate-heats-up-holding-the-police-accountable-2/.

transparency, minimizing psychological violence and rigid lines of questioning."[118]

Indeed, an 'External Audit of the VioGén System' by Eticas Consulting, an algorithmic auditing company, found that *"80% of those interviewed had some kind of problem with VioGén, which generated biased data"*.[119] This audit also revealed that VioGén collects information on victim and aggressor nationality,[120] producing racially biased data, which discriminates against and targets minority ethnic groups. The Ministry of Interior responded that the Eticas report *"lack[ed] academic rigour by basing its study and its conclusions on an insignificant statistical sample of only 31 interviews"*.[121] However, the Ministry's Investigator of Domestic Abuse has confirmed that it will not seek to deploy machine learning in the future, as it recognizes that this can cause problematic results, citing the *"COMPAS"* algorithm as an example.[122] This illustrates that police and law enforcement in Spain may be adopting a somewhat cautious approach with respect to their use of big data and algorithms.

Certain sources indicate that the Spanish police and the Spanish civil guard already make use of certain AI-based tools for face recognition. The Spanish Ministry of Interior intends to use and is already experimenting with the algorithm *"ABIS"* which is expected to be used to identify suspects from a database of filed photographs. The algorithm provides a percentage score based on whether the features of the face in the image match those stored on the database. If the algorithm reveals a 100% match between the suspect in question and the photograph on file, it is regarded as a plausible match to the relevant person. The media and other experts have expressed serious concerns about the planned use of this AI. They argue that this type of tool, from a practical perspective, may cause mass surveillance and loss of anonymity and produce a high number of false positives. Secondly, they suggest that this type of system may violate expected EU legal frameworks on the use of AI.

vi. The UK

In the UK, most regulations are non-statutory. Additionally, the UK has passed the Data Protection Act 2018. The UK DPA, Part 3, governs the processing of personal data for 'law enforcement purposes' by police and criminal justice agencies.

All processing of personal data by the police and criminal justice agencies for any

[118] Carlos de Castillo, 'Las víctimas denuncian fallos en VioGén, el algoritmo contra la violencia de género', El Diario, 10 March 2022, https://www.eldiario.es/tecnologia/victimas-denuncian-fallos-viogen-algoritmo-violencia- genero_1_8815201.html.

[119] Manuel Pascual y Isabel Valdes, VioGén: visita a las tripas del algoritmo que calcula el riesgo de que una mujer sufra violencia machista', El Pais, 10 04 2022 https://elpais.com/tecnologia/2022-04- 10/viogen-visita-a-las-tripas-del-algoritmo-que-calcula-el-riesgo-de-que-una-mujer-sufra-violencia- machista.html?event_log=oklogin.

[120] Fundacion Ana Bella y Eticas, 'Las víctimas denuncian fallos en VioGén, el algoritmo contra la violencia de género' 10 March 2022 https://eticasfoundation.org/wp-content/uploads/2022/03/ETICAS- FND-The-External-Audit-of-the-VioGen-System.pdf.

[121] See footnote 25.

[122] See footnote 26.

'law enforcement purposes'[123] must adhere to the following 'law enforcement data protection principles':

- lawful (i.e. based on law) and fair. Personal data may be processed only if it is necessary for the performance of a task carried out for law enforcement purposes by a competent authority or based on an individual's consent.
- specified, explicit, and legitimate. The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate. Personal data collected must not be processed in a manner that is incompatible with the purpose for which it was originally collected.
- adequate, relevant and not excessive in relation to the purpose for which it is processed.
- accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data which is inaccurate is erased or rectified without delay.
- kept for no longer than is necessary for the purpose for which it is processed. Appropriate time limits must be established for periodic review of the need for continued storage for law enforcement purposes.
- appropriate technical or organizational measures must be applied to personal data. There are additional obligations on competent authorities in relation to 'sensitive processing', i.e. processing of *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"*.

Part 3 of the UK DPA sets out various rights of data subjects, which include the 'right not to be subject to automated decision-making'. A competent authority may not make a significant decision (which is a decision that produces an adverse legal effect or significantly affects an individual) based solely on automated processing unless it is required or authorized by law. If such a decision is required or authorized by law, the competent authority must notify the individual. After that notification, the individual has one month to request the competent authority to either take a decision that is not based solely on automated decision-making, or request the reconsideration of the original decision.

d. Good practices

Belgium

- **Data Protection Act**: This act ensures compliance with the GDPR and the LED, providing robust safeguards for personal data processing by law enforcement authorities.
- **Supervisory Authorities**: The establishment of a supervisory authority

[123] 'Law enforcement purposes' are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

for processing personal data by police agencies ensures oversight and accountability.

France

- **Internal Security Code (ISC)**: This code provides detailed regulations for the use of video protection systems and mobile cameras by public authorities.
- **PARAFE System**: The Rapid Automated Border Crossing system uses facial recognition and strongly emphasizes user consent and transparency.

Germany

- **Federal Data Protection Act (BDSG)**: Complements the GDPR and LED, providing a comprehensive legal framework for AI in policing and criminal justice.
- **Hambach Declaration**: Outlines data protection requirements for AI, emphasizing the need to prevent discrimination and ensure transparency and accountability.

Poland

- **Police Services Act**: Outlines the management and supervision of police information systems, providing a basic framework for data protection in law enforcement.
- **Constitutional Privacy Protections**: Articles in the Polish Constitution guarantee the protection of personal data and privacy rights, laying a foundation for further regulatory development.

Spain

- **Constitutional Laws**: Implementation of the GDPR and LED through Constitutional Laws 3/2018 and 7/2021 provides a strong legal basis for data protection in law enforcement.
- **Automated Decision-Making (ADM)**: Law 40/2015 regulates ADM processes in public administration, ensuring oversight and accountability in automated actions.

United Kingdom

- **Data Protection Act 2018**: Complements the GDPR, providing a comprehensive framework for the lawful and fair processing of personal data by law enforcement.
- **Equality and Human Rights Commission**: Enforces equality and human rights laws, focusing on ensuring non-discriminatory use of AI and big data in law enforcement.

e. Lack of regulation

Belgium

- **Facial Recognition**: There is no specific regulation for the use of surveillance cameras incorporating facial recognition technology, leading to potential privacy and discrimination concerns.

France

- **Broad Surveillance**: Despite stringent measures, ongoing debates and legislative changes indicate a need for clearer regulations to address the broad use of AI in surveillance and law enforcement.

Germany

- **Fragmented State Laws**: The diverse legal frameworks across different states create inconsistencies in the application of AI regulations, complicating nationwide enforcement and oversight.

Poland

- **Comprehensive AI Regulation**: There is a significant gap in specific regulations addressing the use of AI in criminal justice and law enforcement, leading to potential risks of misuse and insufficient safeguards for individual rights.

Spain

- **Transparency and Public Information**: Public bodies rarely publish detailed information on ADM systems, leading to a lack of transparency and potential public distrust.
- **Algorithmic Profiling**: Criticisms of the VioGén system highlight the need for clearer regulation and safeguards related to biased data and discriminatory practices.

United Kingdom

- **Non-Statutory Regulations**: Many regulations are non-statutory, leading to potential inconsistencies and gaps in enforcement.
- **Comprehensive AI Laws:** There is a need for more detailed and specific laws addressing the full spectrum of AI applications in law enforcement and criminal justice.

5. Safeguards and protection mechanisms

a. Belgium

Belgium has established a separate supervisory authority in line with the LED for the processing of personal data by police authorities. Pursuant to the Protection of Natural Persons with Regard to the Processing of Personal Data (known as the Data Protection Act or the DPA), this authority's competence is limited to the Belgian police agencies, the general oversight agency of law enforcement, the

Passenger Information Unit, and the taxation administration.[124]

The DPA sets out a specific procedure for actions for injunctions that can be initiated by the data subject or by the Data Protection Authority. These claims should be brought before the President of the Court of First Instance except when personal data is processed in criminal investigations or procedures. There is no single court with territorial competency to hear these claims.[125] The action for an injunction must be brought by means of an adversarial application in accordance with articles 1034ter to 1034sexies of the Belgian Judicial Code. By way of derogation from article 624 of the Belgian Judicial Code, the action may be brought, at the option of the plaintiff, before the President of the Court of First Instance of the domicile or residence of the plaintiff, if the plaintiff, or at least one of the plaintiffs, is the person concerned. Alternatively, it may be brought before the President of the Court of First Instance of the domicile or residence, registered office or place of business of the defendant or one of the defendants, and/or the place or one of the places where part or all of the treatment is carried out. Where the defendant has no domicile, residence, registered office or place of business in Belgium, the action may be brought before the President of the Brussels Court of First Instance. An action based on Article 209 is brought at the request of the person concerned or the competent supervisory authority.[126]

Where an individual is of the view that their personal data has been processed in breach of data protection regulations, they can lodge a complaint before the BPDA.[127] The BDPA also gives data subjects the possibility of submitting a request for mediation or a request for information.[128] The DPA provides guidance for individuals when a breach is suspected.

The DPA also provides a legal basis that allows a body or organization to represent the data subject upon its request if it was founded in accordance with Belgian law. Belgian law requires the body or organization to have legal personality and public interest objectives. Furthermore, it must demonstrate that it has been working in the field of personal data for at least three years.[129]

As such, in September 2022, the Ministerial Decree appointed privacy activist group NOYB as the first privacy and data protection-related qualified entity under the collective redress scheme of the Belgian Code of Economic Law. NOYB

[124] Protection of Natural Persons with Regard to the Processing of Personal Data (30 July 2018), Article 71.

[125] Protection of Natural Persons with Regard to the Processing of Personal Data (30 July 2018), Articles 211(3) and 209.

[126] Protection of Natural Persons with Regard to the Processing of Personal Data (30 July 2018), Article 210.

[127] “Wat doe je bij misbruik?”, Gegevensbeschermingsautoriteit, https://www.gegevensbeschermingsautoriteit.be/burger/privacy/wat-doe-je-bij-misbruik.

[128] “ Introduire une plainte”, Autorité de protection des données, https://www.autoriteprotectiondonnees.be/citoyen/agir/introduire-une-plainte.

[129] Protection of Natural Persons with Regard to the Processing of Personal Data (30 July 2018), Article 220(2).

can file representative actions in Belgium and claim damages for users for the violation of various laws including data protection legislation.

This study was unable to find any examples of enforcement of rights against the police or criminal justice authorities arising from the DPA.

Public or administrative law

Individuals or groups have various recourses to challenge or make a claim against Belgian police or government decisions related to big data, automated and algorithmic decision- making and/or artificial intelligence systems. These include:

- Lodging a complaint with the Comité P and supervisory authority on police information (COC) via the relevant forms or contact details on their website.[130] The websites do not set out prescriptive requirements for such complaints, but as a matter of general practice, the complaints should set out all salient details and, where possible, the alleged breach of the relevant rule. The COC is an independent federal parliamentary institution that monitors the police to ensure that they comply with appropriate legislation for the use of information and data. Comité P is charged with supervising the overall functioning of the police services.
- Lodging a complaint against the Directorate of Police Information and ICT Resources who are tasked with, amongst other things, managing information on legal advice and regulations via the 'file a complaint' form on their website. This is available in Dutch, French or German.[131]
- Access to the Belgian courts, although this will likely require the support of a lawyer or expert.

The General Inspectorate of the federal and local police are also responsible for investigating the services of the federal and local police. However, this is not a process that can be triggered by an individual.

Article 47 of the Police Services Act provides that the Belgian State is liable for the damage caused by the police and their agents. The municipality is the relevant body liable for such damages when the local police are involved.

Depending on the route taken and the extent of escalation of the complaint, it is clear from available documentation that immediate supervisory authorities can review decisions and the application of applicable legislation. In more serious cases, matters can be escalated to the Belgian courts, and eventually the European Court of Human Rights.[132]

[130] Supervisory Body for Police Information, https://comitep.be/lodge-a-complaint.html and https://www.controleorgaan.be/en/contact.

[131] Police online reporting, https://www.police.be/police-on-web/en.

[132] Bouyid v Delgium (Application no. 23380/09) and Missaoui and Akhandaf v Belgium (communicated case).

Equality and anti-discrimination

In relation to claims based on infringements of equality and anti-discrimination rights, as set out under Section 2.e, possible mechanisms include:

- **Filing a complaint**: the Anti-Discrimination Act provides victims with the right to file a complaint with the competent authorities, such as the Centre for Equal Opportunities and Opposition to Racism ('UNIA') and seek compensation for damages suffered. UNIA is a public body that informs individuals concerning the scope and the content of their rights, and may help to lodge complaints. UNIA can opt for negotiation or conciliation, or a transfer of the case to a competent court.[133] Institutions, associations, and organizations whose statutory aim is to combat discrimination may also file a complaint against discrimination. A lawsuit can only be brought if the victim of discrimination is identifiable, and consent is provided by the person concerned.[134] The burden of proof is placed on the alleged perpetrator to prove that the discrimination did not occur.[135]
- **Constitutional Law**: the Belgian Constitution provides victims with the right to file a complaint with the Constitutional Court if their rights have been violated.
- **European Court of Human Rights**: if an individual has exhausted all domestic remedies and still believes that their rights have been violated, they can bring a case before the European Court of Human Rights.
- **Class Actions**: in principle, class actions are not permitted under Belgian law. For actions to be admissible, the claimant must fulfil the 'personal interest' requirement.[136] As such, qualified organizations can seek injunctive relief against practices that infringe on non-discrimination laws.

Possible remedies may include:

- Racism and Xenophobia Law, Anti-Discrimination Act and Gender Law all allow for compensation for damages in case of discrimination, depending on the circumstances. They also enable protection against dismissal and any other detrimental measure related to the filing of a motivated complaint for discrimination.
- Specifically, under the Anti-Discrimination Act, victims of discrimination can seek compensation for material and moral damages, including compensation for financial losses, damages for pain and suffering, and damages for loss or future opportunities.[137] It also provides for injunctive relief, which can require the perpetrator to stop the discriminatory behaviour. Penalties and sanctions include fines and imprisonment.[138]

[133] Racism and Xenophobia Law, Article 31 and Anti-Discrimination Act, Article. 19 et sec.

[134] Anti-Discrimination Act, Articles 30 and 31.

[135] Anti-Discrimination Act, Article 17.

[136] Belgian Judicial Code, Articles 17 and 18.

[137] Anti-Discrimination Act, Article 18.

[138] Anti-Discrimination Act, Articles 22 to 28.

b. Germany

Under Article 18 of the GDPR, data subjects have the right to restrict processing if the data is inaccurate, the processing is unlawful, or personal data is no longer needed for its original purpose.

Under Article 21 of the GDPR, data subjects have the right to object to certain types of processing. Specifically, they have the right to object to processing based on legitimate interests (Article 6(1)(f) GDPR), on public interest (Article 6(1)(e) GDPR), or for direct marketing purposes.

Under Article 22 of the GDPR, data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning them or similarly significantly affects them.

Also, data subjects have the right to restrict processing under Section 58 BDSG. However, this right is only applicable if the data subject exercises their right to rectification and the accuracy or inaccuracy of the data cannot be ascertained.

The right to restrict processing is also applicable where the data subject exercises their right to erasure, and the controller selects restriction under Section 58(3) BDSG.

As mentioned above, BDSG does allow for decisions based solely on automated processing, including profiling under the prerequisites described above.

c. Poland

In Poland it is possible to exercise the right not to be subject to automated decision-making, including profiling. Decisions which produce legal effects concerning the individual or similarly significantly affects the individual are only permitted when:

- necessary for entering into or performing a contract.
- authorized by EU or Polish law.
- the individual has given their explicit consent.

The right not to be subject to automated decision-making in Poland does not deviate from the provisions of the GDPR. As described above, the Police Directive does not allow for fully automated decision-making but, unlike the GDPR, it does not detail when such decision- making would be permitted.

In Poland, there are no known sanctions such as fines or enforcement activities related to big data, databases, algorithms, automated systems, or AI.

d. Spain

The Spanish regulatory authorities have powers to supervise compliance with data protection regulations, and various sanctions apply, which also apply to police and criminal justice authorities. For data subjects, avenues of redress exist under general principles of Spanish law. There do not appear to be any specific procedures or redress mechanisms to challenge the lawfulness of how big data, automated and algorithmic decision-making and AI systems are used by police and criminal justice authorities. This includes third parties operating on their behalf or alongside them. Under general principles of Spanish law, remedies exist under constitutional protection mechanisms and equality and non-discrimination infringements.

Constitutional Law 7/2021, implementing the LED, classifies data protection infringements as minor (Article 60), serious (Article 59), or very serious (Article 58) and specifies that the statutory limitation period ranges from six months to three years, depending on the classification of the infringement. Article 62 sets out that sanctions range from one to three years, respectively, with fines categorized accordingly. The levels set for minor infringements are €6,000 - €60,000, for serious infringements €60,001 – €360,000, and very serious infringements €360,001 – €1,000,000.

Article 49 of Constitutional Law 7/2021 provides that the supervisory authorities responsible for supervising the application of the GDPR (i.e. AEPD, or relevant regional data protection authority, such as the Catalan Authority for Data Protection, ("**APDCAT**")) are also competent to monitor the application of the LED. Indeed, AEPD has the authority to carry out inspections and investigations to verify compliance with data protection regulations. It can impose administrative fines and penalties for violations.

In relation to this, since May 2018, AEPD has issued 33 decisions concerning matters within the scope of the LED on the basis of the former Spanish Data Protection Act. These decisions correspond to complaints lodged by data subjects in relation to the exercise of data protection rights, including access, rectification and erasure. Complaints linked to certain uses of data (i.e., relating to video surveillance or publication of personal data on the internet) may be lodged on the AEPD website. The AEPD complaints system is not limited to certain categories of data breaches, as there is a catch-all option to file a complaint about "any other data breach".

Individuals may claim damages arising from the breach of their data protection rights before the civil courts. Claims for civil damages usually involve pecuniary or moral damages, or both, linked to the violation of honour (such as the improper disclosure of private information) and privacy rights (such as the dissemination of private images).

Damages have infrequently been granted to date and have not exceeded €3,000 (with limited exceptions such as one awarding €20,000).

Spanish Agency for the Supervision of Artificial Intelligence ("AESIA")

Spain has also announced the creation of a national agency to enforce, supervise and regulate AI, which will be known as the Spanish Agency for the Supervision of Artificial Intelligence ("**AESIA**"). This agency will function independently from the government and will oversee private and public sector algorithms. On 22 August 2023, the Council of Ministers adopted the AESIA statute, which empowers AESIA to oversee and enforce AI regulations brought about by the entry into force of the EU AI Act. The precise mandate and powers of AESIA are still being finalized by the Spanish government.[139]

e. The UK

The Equality and Human Rights Commission (Commission) is a regulatory body responsible for enforcing the Equality Act 2010 and the Human Rights Act 1998. The Commission publishes general guidance on implementing the requirements of the two acts. It can also use courts and tribunals to obtain binding judgments against organizations that fail to comply.

The Commission has so far focused on big data and AI and plans to focus on automated decision-making algorithms in the future as part of its three-year plan 2022-2025. When it comes to AI and big data, the Commission issued a checklist[140], which focuses on ensuring equality. The checklist requires the organization to review positive and negative impacts of AI on people with different protected characteristics and to keep records of the impact assessment. It requires organizations to publish the results of the impact assessment for transparency and, monitor impact and amend the AI as necessary to ensure equality.

The Equality and Human Rights Commission published a report[141] on the use of AFR and predictive algorithms in policing in England and Wales. The report pointed out several serious breaches of laws. For example, as a result of an investigation, the Information Commissioner found that a database and profiling tool used by the Metropolitan Police Service (MPS) to identify potential victims and perpetrators called the 'Gangs Matrix' failed to comply with multiple data protection laws.[142]

f. Policies, strategies and reports

In this section, we include examples of policies, national strategies, and reports that assess the use of AI by criminal justice and police authorities. Not all countries have developed detailed information on this topic, so information can be sporadic.

[139] Pablo Jiménez Arandia, 'What to expect from Europe's first AI oversight agency', Algorithm Watch, 1 February 2023, https://algorithmwatch.org/en/what-to-expect-from-europes-first-ai-oversight-agency/.

[140] The Equality and Human Rights Commission, the AI checklist.

[141] The Equality and Human Rights Commission, Civil and political rights in Great Britain, March 2020.

[142] Information Commissioner's enforcement notice to the Metropolitan Police, November 2018.

i. France

The National Assembly's Committee on Constitutional Law, Legislation and the General Administration of the Republic published a report, Parliamentary Report No. 1089 dated 12 April 2023, on challenges related to the use of security images in the public domain for the purpose of combatting insecurity.[143] The report notes that the intrusion of AI into security technologies raises challenges, which require questioning the usual balance between the imperative for security and the need to protect fundamental freedoms (notably the right to privacy).

The report makes 41 recommendations which include those related to the use of smart cameras, automated processing and facial recognition. It remains to be seen whether these recommendations will be implemented. A parliamentary report is not binding on Members of Parliament. Rather, it is a working document, which may lead to a discussion in a public session and may inform the work of the parliament and government when preparing new bills.

CNIL

On 15 November 2019, CNIL published a report on facial recognition, which discusses risks and requirements associated with the use of AI technologies. It addresses appropriate guarantees for the protection of privacy and personal data, as well as suggesting steps to inspire trust in any system to be implemented.[144] CNIL notably identified the following risks:

- ***Risks associated with the sensitive nature of data***

CNIL stresses that biometric data constitutes sensitive data under the Data Protection Act and that the misappropriation or misuse of this data may lead to particularly severe consequences for individuals. These can include removal of access to a service or a location and/or identity theft.

- ***Risks associated with the contactless and potentially omnipresent nature of the technology***

CNIL points out that facial recognition data is potentially available everywhere, i.e. this data can be collected and stored in a multitude of databases. This dissemination of data also takes place in a context of frequent self-exposure on social networks as well as overlap between domestic, private and public use of data.

In addition, facial recognition is a 'contactless' technology meaning that it can operate without the individual being aware of it.

[143] Assemblée Nationale, Commission des lois constitutionnelles, de la législation et de l'administration générale de la République (12 April 2023), *Report No. 1089 on the challenges of using security images in the public domain to combat insecurity* (available at: https://www.assemblee- nationale.fr/dyn/16/rapports/cion_lois/l16b1089_rapport-information).

[144] CNIL (15 November 2019), Facial recognition: for a debate living up to the challenges (available at: https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux).

- **Risks linked to the costs and reliability of technology**

Facial recognition is based on statistical estimates and is therefore fallible.[145] There is a risk of false negatives and false positives. Variations in performance can have very serious consequences on those misidentified.

Current facial recognition technology is also subject to significant biases. For example, experiments have shown that error rates committed by facial recognition algorithms can vary according to gender or skin colour.[146]

Different accuracies of facial recognition in different demographic groups can result in a lack of reliability of facial recognition technology.

- ***Risks relating to broad surveillance, societal and ethical risks***

CNIL notes that facial recognition can interact with many video devices, which are available in everyday life. In today's digital environment, where people's faces are readily available in databases and captured by cameras, facial recognition has become a particularly ubiquitous and intrusive tool. The most advanced uses of facial recognition, therefore, present a clear risk of undermining anonymity in public.

According to CNIL, facial recognition has created a paradigm shift. The shift they describe is from surveillance targeted at specific individuals to surveillance of everyone with the aim of identifying certain individuals.[147]

On 19 July 2022, following a public consultation, CNIL published a position paper on smart cameras.[148] CNIL noted that smart cameras pose new risks to rights and fundamental freedoms, as the uncontrolled widespread use of such technologies, which are intrusive by nature, could lead to widespread surveillance and analysis in public, which could, in turn, modify people's behaviour.

CNIL stressed that anyone willing to use smart cameras should comply with the principles laid down in data privacy laws and stressed that certain technologies, notably those implemented for general administrative or judicial police purposes, should be authorized by law. In this respect, and at the time of the publication of their paper, the law did not allow police forces to connect automatic analysis

[145] "Facial Recognition Debate: Living Challenges." CNIL - Commission Nationale de l'Informatique et des Libertés, www.cnil.fr/en/facial-recognition-debate-living-challenges.

[146] The 2018 Gender Shades project found that facial recognition performed the worst for dark skinned females with a 34% error rate compared to light skinned males with a 1% error rate. "Study Finds Gender and Skin Type Bias in Artificial Intelligence Systems." MIT News, 12 Feb. 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[147] **Lúcia, Raposo**. The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal, (01 June 2022) available at https://link.springer.com/article/10.1007/s10610-022-09512-y.

[148] CNIL (July 2022), *"Smart" or "augmented" cameras in public spaces* (available at: https://www.cnil.fr/fr/cameras-dites-augmentees-dans-les-espaces-publics-la-position-de-la-cnil).

devices to video-protection cameras.

CNIL also noted that the use of smart cameras often leads to a reduction in data subject rights, especially the right to object to the processing of their personal data. CNIL reaffirmed that the right to object can only be limited where data processing is carried out for statistical purposes and/or the right has been waived by legal or regulatory provisions.

CNIL decided to make the use of smart cameras one of its priorities for investigation in 2023.[149]

ii. Germany

The Federal Government (Bundesregierung) introduced the "Artificial intelligence strategy of the federal government"[150] in November 2018. In December 2020, the Federal Government published an update of the strategy to focus its measures with regard to new developments in the field of AI.

One identified priority is the adjustment of the legal framework. The Federal Government has stated that it will review and, if necessary, adapt the legal framework for algorithm and AI decisions, services, and products to ensure effective protection against bias, discrimination, manipulation, or other abusive use.[151]

In the Hambach Declaration on Artificial Intelligence, the Data Protection Conference set out seven data protection requirements for the general use of AI. First, the Data Protection Conference clarified that possible discrimination through AI results violates the rights of the data subject and, among others, violates provisions of the GDPR. Before implementing AI systems, it is therefore necessary to conduct an assessment of the risks to the rights and freedoms of individuals. This is done with the aim of safely preventing even hidden discrimination through effective countermeasures. During the deployment of AI systems, continuous monitoring of risks is necessary. In addition, it is necessary to clarify and clearly communicate the responsibility for the use of an AI system. Stakeholders must take the necessary steps to ensure lawful processing, data subject rights, security of processing, and controllability of the AI system.[152] The BfDI has also published a paper on the use of artificial intelligence in law

[149] CNIL (21 March 2023), *Priority topics for investigations in 2023: "smart" cameras, mobile apps, bank and medical records* (available at: https://www.cnil.fr/en/priority-topics-investigations-2023-smart-cameras-mobile-apps-bank-and-medical-records).

[150] Federal Government of Germany, `Artificial intelligence strategy`, 2018, https://www.ki-strategie- deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf&cid=729.

[151] Federal Government of Germany, https://www.ki-strategie-deutschland.de/home.html.

[152] Data Protection Conference, `Hambach Declaration on artificial intelligence`, 2019, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/97DSK_HambacherErklaerung.pdf?__blob=publicationFile&v=5.

enforcement and security.[153]

Abida[154] (Assessing Big Data) is an interdisciplinary project funded by the Federal Ministry of Education to evaluate societal opportunities and risks of generating, linking and analyzing large amounts of data. Abida published an expert opinion on "Ethical Standards for Big Data and their Rationale"[155]. One of their key findings was that ethical standards should be regulated in law.

The State Office Berlin for Equal Treatment – Against Discrimination (Landesstelle für Gleichbehandlung - gegen Diskriminierung) published a paper on algorithms and the right to digital equality.[156] Their findings are that algorithmic systems are never neutral, because the learning data of such algorithms is already characterized by discriminatory structures and asymmetrical power relations.

Other laws

While there are no other types of laws or policies that regulate or limit the use of big data and databases, algorithms, automated systems or AI, the work of the German Ethics Council is noteworthy. The German Ethics Council (Deutscher Ethikrat) published an extensive report on the challenges of Artificial Intelligence.[157] The report partially covers the use of AI by law enforcement agencies. The key findings are:

- Algorithmic systems can be useful in the fight against crime. However, risks associated with such systems, especially if there are errors or bias, must be monitored. Appropriate technical and organizational measures must be implemented to avoid such errors and bias.
- Predictive policing must respect the protection of personal data and privacy. The development and use of algorithmic systems should follow high requirements regarding transparency.
- Rights of access and objection by data subjects must be guaranteed when algorithmic systems are used.
- Individuals who manage algorithmic systems must have the necessary competencies.

[153] Federal officer for Data Protection and Freedom of Information, `Thesis paper of the BfDI on the topic: Use of Artificial Intelligence in the area of law enforcement and security`, 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/2_KI-Strafverfolgung/Positionspapier-KI-Erstversion.pdf? blob=publicationFile&v=2.

[154] Abida (Assessing Big Data), https://www.abida.de/en.

[155] Abida, `Expert Opinion on Ethical standards for Big Data and their Rationale `, 2019 http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Ethische%20Standards.pdf.

[156] State Office Berlin for Equal Treatment – Against Discrimination, `Algorithms and their discrimination risk`, 2019, https://www.berlin.de/sen/lads/_assets/ueber-uns/materialien/algorithmendiskriminierungsrisiko_bf.pdf.

[157] German Ethics Council, `Report on the challenges of Artificial Intelligence`, 2023 https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf.

- Quality criteria related to accuracy, error prevention and bias must be defined as mandatory and transparent.

iii. Poland

Artificial intelligence policy

In April 2023, during a conference on 'AI in the Polish Court System' the Attorney General and Vice-Minister of Justice expressed views that AI and algorithms help automate the legal system to improve its efficiency. The Attorney General noted that every third case is now being resolved electronically. He emphasized that any changes must be implemented in line with due process.[158]

Additionally, an artificial intelligence tool is being trialed in certain prisons to identify potentially dangerous or suspicious activities. The tool utilizes specially developed algorithms to automatically detect and make rational predictions about future events. When a situation arises within the prison that the system identifies as an anomaly, it will promptly signal this with both visual and auditory alerts on the monitors. Analogue cameras, which are still present in some prisons, continue to provide additional feed.[159]

iv. Spain

The National Artificial Intelligence Strategy has published its strategic lines of action in respect of AI targets to be achieved by 2025.[160] In particular, action six seeks to "establish an ethical and regulatory framework that reinforces the protection of individual and collective rights, to guarantee inclusion and social wellbeing". The National Artificial Intelligence Strategy will also scrutinize those "uncertainties owing to the ethical, legal, social and economic implications of AI", and "evaluate if the current ethical and regulatory framework preserves the rights of the citizen in a digital world and prioritizes ethical and democratic objectives".

The Spanish Government released its National Artificial Intelligence Strategy in December 2020 to develop a policy framework defining the various actions that the government needs to undertake to facilitate the development and

[158] Ministry of Justice, "Sztuczna inteligencja w służbie wymiary sprawiedliwości – konferencja Ministerstwa Sprawiedliwości" 17 April 2023, Accessed September 21, 2023. https://www.gov.pl/web/sprawiedliwosc/sztuczna-inteligencja-w-sluzbie-wymiaru-sprawiedliwosci--konferencja-ministerstwa-sprawiedliwosci.

[159] Polskie Radio Lublin, „Lubelskie: sztuczna inteligencja pomoże pilnować więźniów" 1 July 2021, Accessed September 21, 2023. https://radio.lublin.pl/2021/07/lubelskie-sztuczna-inteligencja-pomoze-pilnowac-wiezniow/; „Sztuczna Inteligencja pomoże służbie więziennej" 26 October 2022, Accessed September 21, 2023. <https://radio.lublin.pl/2022/10/sztuczna-inteligencja-pomoze-sluzbie- wieziennej/>; Frączak. Mikołaj, „Sztuczna inteligencja zadba o bezpieczeństwo w więzieniach" 27 December 2023, Polityka Bezpieczeństwa, Accessed September 21, 2023. https://www.politykabezpieczenstwa.pl/pl/a/sztuczna-inteligencja-zadba-o-bezpieczenstwo-w-wiezieniach.

[160] Estrategia Nacional de Inteligencia Artificial, España Digital 2025, Noviembre 2020 https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/021220-ENIA.pdf.

deployment of AI in the economy and society.[161]

It does not appear that there are any specific procedures or redress mechanisms to challenge the lawfulness of how big data, automated and algorithmic decision-making systems and AI systems are used by police and criminal justice authorities. This includes any third parties operating on their behalf or alongside them. However, there are some general principles under Spanish law that may enable individuals concerned to challenge such measures under general administrative laws.

For example, Law 39/2015[162] on Common Administrative Procedure for Public Administration states that citizens can present claims directly to the public administration that, according to that individual, has violated his or her rights. A specific part of this law is dedicated to the procedure of remedies. In addition, Law 2/1986[163] on Security Institutions and Forces states that rules on remedies also apply in case of violations of fundamental rights by the police. Different phases of this type of procedure exist. Only once the given procedure is exhausted, can an entity appeal to the respective administrative courts.[164]The appropriate proceedings before the Spanish administrative courts are stipulated in Law 29/1998[165] regulating the contentious-administrative jurisdiction.

Pursuant to the constitution, legal remedies in case of rights violations are awarded by national courts (civil, criminal, labour, and administrative) as well as the Constitutional Court, which becomes relevant once an appeal on the grounds of unconstitutionality is presented.

The procedures to challenge the lawfulness of administrative action in Spain, generally do not require the involvement of lawyers. However, it is likely that dealing with these cases will involve a level of complexity from a legal perspective. As a result, the involvement of a lawyer will in most cases make sense. As for the redress that can be obtained, the potential outcomes vary depending on the circumstances and the relief sought. Possible forms of redress include:

- Review or overturn the administrative decision: If successful, the administrative decision can be reviewed or overturned, leading to a more favourable outcome for the individual or group challenging it.
- Financial compensation: In some cases, individuals who have suffered harm or damages due to an unlawful administrative decision may be entitled to financial compensation.[166]This is typically determined by the courts based on

[161] Hogan Lovells, 'Spain to create Europe's first supervisory agency for artificial intelligence' Lexology 13 January 2022 https://www.lexology.com/library/detail.aspx?g=d2d01036-bbdf-451a-b3e7-485f51148b76.

[162] Law 39/2015, 1 October 2015.

[163] Organic Law 2/1986, 13 March 1986.

[164] 'Artificial Intelligence, Big Data and Fundamental Rights, Country Research Spain, 2020 https://fra.europa.eu/sites/default/files/fra_uploads/fra-ai-project-spain-country-research_en.pdf.

[165] Law 29/1998, 13 July 1998.

[166] Law 40/2015, 01 October 2015.

the evidence presented.

• Injunction or specific action: In certain situations, individuals may seek injunctive relief to prevent the administrative authority from taking a certain action or to compel them to carry out a specific action required by law.[167]This study has not been able to find any examples where specific action has been applied to police use of data.

g. Application

Some limited examples of how rules are applied to specific cases, which help to measure their effectiveness, are presented below.

i. Belgium

Facial recognition

One of the more prominent examples of the use of intelligent systems by the police force in Belgium was the use of automated facial recognition surveillance systems during a testing phase at Brussels Airport.[168]

While the COC ruled in two circumstances that the use of facial recognition software and creation of related databases is not in line with police powers under the Police Services Act, some intelligent camera systems continue to be used (in compliance with the relevant legal requirements). For example, in the Flemish town of Kortrijk, intelligent camera systems can detect certain elements or characteristics (e.g., the colour of a bag or an individual's attire) but not a person's identity.[169]

Currently, there appear to be no final court rulings that oppose the legality of these predictive policing systems in principle. Rather, there have been court decisions on specific actions and consequences of these systems. For example, in 2017, an interim decision by the Brussels Court of First Instance invalidated the preventive screening[170] of the three ticket holders to the 2017 Tomorrowland festival in Boom, Belgium. The organizers of Tomorrowland had been ordered by the local mayor to disclose the personal data of all Tomorrowland ticket holders and personnel to the police. The police then matched this data against the national police database, as well as other databases, to determine whether any of these individuals might pose a risk to public safety during the event. If a

[167] Law 29/1998, 13 July 1998.

[168] Bert Peeters, "Facial recognition at Brussels Airport: face down in the mud", KU Leven, (17 March 2020), https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in- the-mud/.

[169] Gabriela Galindo, "No legal basis for facial recognition cameras at Brussels Airport", The Brussels Times, (10 July 2019), https://www.brusselstimes.com/60362/no-legal-basis-for-facial-recognition- cameras-identity-brussels-airport-intelligent-cameras.

[170] Lucia Greco, "Tomorrowland screened +400k ticket holders and denied access to 38 people!", Night Mag, https://xceed.me/blog/en/tomorrowland-screened-400k-ticket-holders-and-denied-access-to-38-people/.

matched was found, the individual in question was expected to be denied access to the festival.[171]
While the decision was mainly based on the violation of the presumption of innocence and the need for appropriate safeguards, the court explicitly stated in its decision that it did not consider the screening to be illegal in principle. As of the date of this report, this decision has not been published as this was only an interim order.

Belgian data protection authority investigates smart surveillance cameras (2020)

As way of an example of the application of these rules, the Belgian Data Protection Authority ('BDPA') opened an investigation concerning the installation by 'Westtoer' of a network of smart cameras on the Belgian coast to measure crowding.[172]The BDPA learned through the press of the installation.

BDPA investigation asked various questions about this network of smart cameras, including how they ensure the counting of individuals and not their identification. In its decision, BDPA issued a reprimand to Westtoer and imposed several other general corrective measures. The BDPA asserted that, given the high risks to rights and freedoms of individuals, Westtoer must take appropriate measures to ensure data protection and privacy were respected.
The BDPA concluded that the required technical and organizational measures included minimizing the image storage period, blurring images of passers-by, ensuring data security, limiting access to data and only siting cameras in areas of high footfall.[173]

The Belgian police tried to use automated facial recognition surveillance systems during a testing phase at Brussels Airport. These surveillance systems were subsequently banned in[174] the Police Services Act (which generally allows for the use of intelligent cameras[175]) as the creation of a database to compare camera images to existing biometric data was not allowed.

Moreover, a clear legal basis for the use of such systems to identify individuals is required, particularly according to Article 34 of the DPA. According to the COC interim report, there was no such legal basis identified during the testing of automated facial recognition systems at Brussels Airport. Therefore, COC requested that the facial recognition system be temporarily disabled until

[171] Ronny Saelens and Brendan van Alsenoy, "Privacy in Tomorrowland: Brussells court invalidates police screening", KU Leven, (1 August 2017), https://www.law.kuleuven.be/citip/blog/privacy-in-tomorrowland-brussels-court-invalidates-police-screening/.

[172] "Mesure de l'affluence a la cote belge : premiere decision de l'APD sur une mesure Covid-19" (19 February 2021), https://www.autoriteprotectiondonnees.be/professionnel/mesure-de-laffluence-a-la- cote-belge-premiere-decision-de-lapd-sur-une-mesure-covid19.

[173] Ibid.

[174] Bert Peeters, "Facial recognition at Brussels Airport: face down in the mud", KU Leven, (17 March 2020), https://www.law.kuleuven.be/citip/blog/facial-recognition-at-brussels-airport-face-down-in- the-mud/.

[175] Ibid.

appropriate risk and impact analysis related to privacy and personal data protection was submitted. This needed to be accompanied by an adequate and concrete security policy and security plan.[176]

Belgian Police have continued to use facial recognition software, such as 'Clearview AI'.[177] In this regard, COC ruled that the use of Clearview AI lacks the appropriate legal basis and does not comply with the requirements of Article 44/1 § 2 No. 1 of the Police Services Act in relation to the handling of biometric data. In its decision, COC argued (inter alia) that although the Police Service Act allows the processing of biometric data in general, there is no adequate legal basis for the Belgian police to utilize such a form of facial recognition technology.[178]

ii. Germany

The **Federal Constitutional Court** (Bundesverfassungsgericht) ruled in May 2023 that telecommunications surveillance against a person who is not accused is only lawful where it may be assumed, based on certain facts, that they are receiving or transmitting messages intended for or originating from the accused and/or the accused is shown to be using their telephone connection or information technology system. In the case in question, the police had only vague indications of these realities. Therefore, the Federal Constitutional Court considered the telecommunications surveillance to be inadmissible.[179]

In April 2021, the **Federal Court of Justice** (Bundesgerichtshof) confirmed that under the StPO provision, which governs telecommunication surveillance, law enforcement is allowed to monitor and record email accounts.[180]This decision is being criticized by criminal lawyers as they fear that a protected space for communication is unlikely to remain.[181]

[176] Report No. DIO19005 of the Controleorgaan op de Politionele Informatie (16 September 2019).

[177] Agnes Szucs, "Belgian police admit using controversial facial recognition software", Anadolu Agency (11 October 2021), https://www.aa.com.tr/en/europe/belgian-police-admit-using-controversial-facial-recognition-software/2388953.

[178] Report No. DIO21006 of the Controleorgaan op de Politionele Informatie (4 February 2022) available here.

[179] Bundesverfassungsgericht (Federal Constitutional Court), `Decision of March 21, 2023, 2 BvR 0626/20, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/03/rk20230321_2b vr062620.html.

[180] Bundesgerichtshof (Federal Court of Justice), `Decision of April 28, 2021, StB 47/20, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&az=StB%2047/20&nr=118375.

[181] https://www.ferner-alsdorf.de/bgh-bekraeftigt-mail-ueberwachung-ist-durch-%c2%a7-100a-stpo-gedeckt/.

6. Conclusions

To conclude, the regulation of AI in the context of police and criminal justice systems varies significantly across European countries. While the EU Artificial Intelligence Act marks a significant step toward harmonizing AI regulation, there remains considerable divergence in how individual countries implement and enforce these regulations. Countries such as Germany and France have taken proactive steps in creating specific legal frameworks, whereas others, like Poland, lag behind in comprehensive AI regulation.

Germany has integrated the Federal Data Protection Act alongside the GDPR and LED, setting a robust foundation for regulating AI in policing and criminal justice. The use of smart CCTV cameras, automatic license plate reading systems, and automated facial recognition technologies is subject to stringent legal requirements and oversight. However, despite these regulations, the fragmented nature of state laws presents challenges in maintaining uniform standards across the country.

France has established detailed regulations under the Internal Security Code (ISC) and other legislative instruments, such as the Criminal Procedure Code and the 'Olympic Games Law'. These regulations govern the use of video protection systems, mobile cameras, and automated border control systems (PARAFE). The French approach emphasizes transparency, public consent, and stringent safeguards against misuse, but ongoing debates and legislative changes indicate a dynamic regulatory landscape.

Belgium and the UK have also made strides in regulating AI, with Belgium focusing on data protection through the Data Protection Act and the Law Enforcement Directive. The UK GDPR is supplemented by the Data Protection Act 2018, emphasizing the need for lawful, fair, and transparent processing of personal data by law enforcement. However, both countries face challenges in ensuring comprehensive and consistent application of these regulations, particularly concerning the use of predictive policing tools and facial recognition technologies.

Poland represents a contrasting example, with limited specific regulations addressing AI in the criminal justice system. The Police Services Act and other general data protection laws provide a basic framework, but there is a lack of detailed provisions and effective enforcement mechanisms. This gap highlights the need for Poland to enhance its regulatory approach to address the growing use of AI in policing and ensure alignment with broader European standards.

The fragmented nature of existing legal mechanisms across Europe makes it challenging for individuals to understand and invoke their rights effectively. This underscores the necessity for clearer, more cohesive regulations that are accessible to all stakeholders. Continuous monitoring and adaptation of these regulations are essential to address the evolving nature of AI technologies and their implications for human rights and fundamental freedoms.

In conclusion, while significant progress has been made in regulating AI in criminal justice and security contexts, there is still much work to be done to ensure responsible and ethical use of these technologies. Future efforts should focus on enhancing transparency, accountability, and public awareness to build trust in the use of AI. Collaborative initiatives at both national and European levels will be crucial in creating a unified and effective regulatory environment that safeguards human rights while enabling the benefits of AI in maintaining public safety and justice.

7. Recommendations

1. **Adopt a human rights approach**. AI regulation regarding criminal and law enforcement should be grounded in a human rights framework, ensuring that it protects privacy and data, supports a fair trial, and prevents discrimination. This approach should be aligned with international human rights standards.
2. **Establish clear legal frameworks for AI use**. Countries should develop comprehensive legal frameworks that regulate the use of AI by police and criminal justice authorities. These frameworks should include stringent data protection measures, ensure transparency, and require regular audits to prevent and mitigate risks associated with AI technologies.
3. **Implement specific AI regulations**. Germany and France have detailed regulations governing AI in policing, which other countries can emulate. For example, Germany's Federal Data Protection Act, alongside GDPR and LED, provides a robust foundation. France's Internal Security Code and other legislative instruments emphasize transparency and public consent.
4. **Ensure ethical standards and non-discrimination prevention**. AI systems must be designed and implemented with safeguards to prevent discrimination and ensure ethical use. This includes continuous monitoring to detect, prevent, and mitigate any discriminatory effects.
5. **Facilitate redress mechanisms**. Establish clear procedures for individuals to challenge the use of AI by police and criminal justice authorities and seek redress if their rights are violated. This includes providing access to information about how AI systems make decisions and ensuring that victims can contest these decisions in a fair and timely manner.
6. **Training and education.** Law enforcement and judicial personnel must be trained in the use of AI and its legal implications, based on a human rights approach.

fairtrials.org

Fair Trials

Fair Trials
Avenue Brugmann 12A
1060 Saint Gilles
Brussels
Belgium

+32 (0)2 894 99 55

@fairtrials in @fairtrials f Fair Trials

Fairness, equality, justice