EDRi

EUROPEAN DIGITAL RIGHTS

EIJI

# THE RISE AND RISE OF BIOMETRIC MASS SURVEILLANCE IN THE EU

## A LEGAL ANALYSIS OF BIOMETRIC MASS SURVEILLANCE PRACTICES IN GERMANY, THE NETHERLANDS, AND POLAND

By Luca Montag, Rory Mcleod, Lara De Mets, Meghan Gauld, Fraser Rodger, and Mateusz Pełka

# INDEX

### About the Edinburgh International Justice Initiative (EIJI)

The Edinburgh International Justice Initiative (EIJI) is a student run initiative that seeks to help institutions working to ensure justice for victims of international crimes and strengthen the international justice system by providing pro-bono legal research assistance that can make a practical difference.

### About European Digital Rights (EDRi)

EDRi is the biggest European network defending rights and freedoms online. The EDRi network is a dynamic and resilient collective of 45 NGOs, as well as experts, advocates, and academics working to defend and advance digital rights across Europe and beyond.

Together, the EDRi network builds a movement of organisations and individuals pushing for robust and enforced laws, informing and mobilising people, and promoting a healthy and accountable technology market.

The EDRi Brussels office lead for this piece of work was Ella Jakubowska, Policy Advisor, with support from Diego Naranjo, Head of Policy.

The EDRi Brussels office would like to express our sincere gratitute to the whole EDRi network, upon whose work this report builds. In particular, we would like to thank the following organisations for making a particular contribution to this report:

- **Bits of Freedom (the Netherlands);**
- **Chaos Computer Club (CCC) (Germany);**
- **Fundacja Panoptykon (Poland);**
- **Electronic Privacy Information Center (EPIC) (International).**

*Brussels, 7 July 2021.*

# INTRODUCTORY NOTE

## Acknowledgements

The team would like to thank **Benedict Coyne**, who provided invaluable support and detailed feedback as the external supervisor on this project. The team would also like to thank **Ella Jakubowska**, our point of contact in EDRi, for clarifying any and all questions, providing us with invaluable guidance throughout, and linking us with important contacts. Finally, the team thanks everyone at **EIJI** for their hard work and diligence in facilitating this project. Thank you all.

## Disclaimer

The EIJI is a student-led body. As we are not lawyers, we are not giving legal advice. Our role is to provide research assistance to EDRi, and thus we do not assume any liability for how this report is used in the future. Furthermore, the EIJI is an apolitical body. The contents of this report are not to be viewed as a political statement nor as a form of advocacy work.

The way this report is used by the EIJI's partners is at their sole discretion and does not reflect the views of the EIJI. Where EDRi has chosen to frame the research within the context of EDRi's advocacy work, this is clearly marked within this report as EDRi's contribution.

## Research Team

**Luca Montag** (Research Team Coordinator) is a fourth year LLB student at the University of Edinburgh with a particular interest in the field of digital rights, employment, and public law. He has been involved with the EIJI since June 2020 as a legal researcher and later as a Research Coordinator.

**Rory Macleod** is in his second year of the accelerated LLB at the University of Edinburgh, having previously completed a degree in Practical Filmmaking at the University of West London. He has a particular interest in constitutional and public law and hopes to pursue a legal career that furthers the public interest in Scotland. He joined the EIJI in October 2020.

**Lara De Mets** is an LLM student at the University of Edinburgh, pursuing a Masters in International Law. She previously obtained an LLB (Hons) degree in Law and Politics from the University of Glasgow. She joined the EIJI in September 2020 and has keen interests in issues surrounding gender (in)justice in peace processes and the Israel-Palestine conflict.

**Meghan Gauld** is a third year International Law and International Relations student at the University of Edinburgh. She is interested in constitutional law, international criminal law, and the law of international trade. She joined the EIJI in September 2020.

**Fraser Rodger** is a third year Law and French LLB student at the University of Edinburgh, with keen interests in international human rights, criminal law, and constitutional law. He joined the EIJI in September 2020 and hopes to qualify as an advocate or barrister.

**Mateusz Pełka** is a third year LLB student at the University of Edinburgh, with a keen interest in European Union law and intellectual property. He joined the EIJI in September 2020 and hopes to pursue a career working for the European Court of Justice in the future.

## Context

### Background

Although surveillance measures have been a part of human history for decades, the digital age has ushered in a myriad of tools and possibilities for the collection, retention, and processing of information which can identify individuals.

The use of biometrics, such as facial features, fingerprints, gait, and vein patterns, has become increasingly more common in recent years. Their use cuts across a wide range of practices and surveillance measures are no exception. It is their use as a mass surveillance tool that is the subject of this report.

## Research task

Our task was to produce country reports on EU member states in respect of biometric mass surveillance practices. The chosen research question to be applied to these reports was a general analysis of the legal basis of various biometric processing activities in the respective country, taking into account multiple deployments in varying levels of detail, in addition to the implications of such activities in International, European, and national law.

Given the breadth of biometric processing activities carried out in each country, as well as the unique legal and political contexts in which they were identified, each country report was structured accordingly.

## Methodology

The countries selected by the team were: Germany, the Netherlands, and Poland. The research team was divided into pairs of researchers who investigated and analysed their assigned countries.

These pairings also ensured that each sub-team had a native speaker correlating with the assigned country. **Luca Montag** and **Rory Macleod** researched Germany, **Lara de Mets** and **Meghan Gauld** researched the Netherlands, and **Fraser Rodger** and **Mateusz Pełka** researched Poland. The research coordinator, **Luca Montag**, oversaw the research from all three countries.

The research was conducted in two phases. The first was the identification of biometric processing activities that fell within the scope of biometric mass surveillance. In identifying the major deployments in each jurisdiction, the team relied on a breadth of sources, including: EU legislation, press statements, government publications, Venice Commission reports, relevant domestic legal acts and judicial decisions, ombudsman reports, academic articles, FOI (freedom of information) requests, and news articles.

The team then analysed the issues arising out of the identified deployments in light of the relevant legal frameworks. These include the domestic law of the relevant member state, comparative law from other states where appropriate, EU law, European Court of Human Rights (ECHR) jurisprudence, and public international law, where applicable.

# LIST OF ABBREVIATIONS

**CCTV –** Closed-Circuit Television
**CEO –** chief executive officer
**CJEU –** the Court of Justice of the European Union
**CIPIT –** Centre for Intellectual Property and Information Technology Law
**DPA –** data protection authority
**DPIA –** data protection impact assessment
**ECHR –** European Convention on Human Rights
**ECtHR –** European Court of Human Rights
**EDPS –** European Data Protection Supervisor
**EU –** European Union
**FOI –** Freedom of Information request (form)
**GDPR –** General Data Protection Regulation
**ICCPR –** International Covenant on Civil and Political Rights
**ID –** identity card
**IP –** intellectual property
**LAN –** local area network
**LED –** Data Protection Law Enforcement Directive
**NGO –** non-governmental organisation
**OHCHR –** United Nations Office of the High Commissioner for Human Rights
**The Charter –** Charter of Fundamental Rights of the European Union
**UDHR –** Universal Declaration of Human Rights
**UK –** the United Kingdom
**UN –** the United Nations
**UNHRC –** United Nations Human Rights Committee

# KEY TERMS

### Biometric Data

Article 4(14) GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images of dactyloscopic data".

### Biometric Processing

Biometric processing comes in many forms, and may be referred to interchangeably as recognition, identification, authentication, detection, or other related terms, as well as (often opaque) ways of collecting and storing biometric data even if the data is not immediately processed, all of which are in scope of this paper.

### Controller

Article 4(7) of the GDPR defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

### Processor

Article 4(8) of the GDPR defines a processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

### Mass Surveillance

Any monitoring, tracking, and otherwise processing of personal data of individuals in an indiscriminate or general manner, or of groups, that is not performed in a specific and lawfully "targeted" way against a specific individual. We note that arbitrarily-targeted surveillance can also be considered a form of mass surveillance given the potential for it to be arbitrarily imposed on any individual without reasonable suspicion.

### Facial Recognition

A type of biometric processing, defined by Article 29 Working Party as the "automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorisation of those individuals," whether or not individuals have consented or have knowledge of its use.

### Dactyloscopy

Identification of a person through the comparison of fingerprints.

### Identification

Distinguishing a person from a larger set of individuals.

### Profiling

Article 4(4) GDPR defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

### Public Spaces

UNESCO defines a public space as "an area or place that is open and accessible to all peoples, regardless of gender, race, ethnicity, age or socio-economic level. [...] In the 21st century, some even consider the virtual spaces available through the internet as a new type of public space that develops interaction". This report includes public spaces like streets, parks, or hospitals, as well as privately-owned but publicly-accessible spaces such as shopping centers, stadiums, public transport, and other public interest services.

### Consent

Article 4(11) GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

### Supervisory Authorities

Article 4(21) GDPR defines a supervisory authority as "an independent public authority which is established by a Member State pursuant to Article 51 [GDPR]".

# FOREWORD

**In May 2020, the EDRi network published our position paper "Ban Biometric Mass Surveillance" in response to the chilling rise of facial recognition and other biometric mass surveillance practices across Europe.**

In that paper and in our policy and advocacy work since, we have demonstrated how any deployment of biometric technologies in publicly-accessible spaces, if used in an indiscriminate or arbitrarily-targeted way, constitutes unlawful mass surveillance – regardless of whether it is police, public administration, or corporations doing so.

We have shown how by definition, **any use of biometrics that could lead to mass surveillance is inherently unnecessary and disproportionate under European human rights law.**

We have also evidenced the vast risks and harms to people's privacy, data protection, equality, non-discrimination, and other fundamental rights that are unduly infringed upon by biometric mass surveillance practices.

This latest research, conducted on behalf of EDRi by independent researchers at the EIJI, demonstrates that **the scale of the problem of abusive and unlawful biometric mass surveillance practices in the EU goes even deeper than we knew.**

In line with wider trends that we have been following across the EU and beyond, these reports on Germany, the Netherlands, and Poland are emblematic of an ideology of mass biometric data collection and processing that is accelerating towards becoming systematic for how people are able to exist in Europe.

Without being willing to have their highly sensitive biometric data captured and processed constantly – and contrary to important principles such as data minimisation as well as legal rules that are supposed to prohibit the unnecessary processing of biometric data - **people across these countries will find it increasingly difficult to access civic services, to travel, and even to go to the shops, without being tracked, profiled, and monitored via their biometric characteristics.**

In both the Netherlands and Germany, **such systems are being used repeatedly for petty and disproportionate reasons, especially given the high level of intrusion that they entail.** The numbers of matches are low and the impact even when matches occur is negligible on public interests. That is to say that **even when they work as intended, these systems are not capable of achieving their stated purpose(s).** As the researchers put it, current practices show that the tools are:

**"[D]eployed less in response to specific and evidentiary threats but rather indiscriminately as a precautionary or deterrent measure."**

Given the requirement for any intrusion into people's rights to biometric data protection to be necessary and proportionate, these abstract and purportedly "preventative" measures show not only a falseness of the presumption that people are safer under systems of biometric mass surveillance, but also link in to the ways in which **justifications of cost and efficiency are proliferating at the detriment of concerns and care for people's fundamental rights.**

Other trends identified include **data protection authorities being hamstrung from enforcing existing protections by a serious lack of resourcing.**

This is exacerbated by the fact that, as EDRi has argued, **existing laws relating to biometric data suffer from serious margins of discretion, loopholes, grey areas, and potential for deliberate misapplications of rules (such as mis-using consent as a legal basis) in ways that are de facto permitting biometric mass surveillance practices in the EU.**

Activities to embed and expand biometric mass surveillance practices have frequently been shrouded in secrecy and labelled as "pilots" in cynical attempts to avoid regulatory scrutiny.

In Poland, the impulse has been less about deploying live facial recognition in publicly-accessible spaces – as this research has shown is common in Germany and the Netherlands – and more to establish databases and infrastructures that could enable and facilitate biometric mass surveillance in the future (exactly as the

research has shown has happened in Germany and the Netherlands in recent years). Furthermore, this research reveals that **the purported justification for including biometric data in national identity cards, such as in Poland and Germany, lacks legitimacy.**

**Furthermore, in both Germany and in Poland, authorities seem to have used the COVID-19 pandemic as a Trojan horse for widening surveillance measures** in ways that are still being seen, despite their justification expiring. For example, police in Poland continue to visit the homes of people subject to the facial recognition 'Home Quarantine' app even after their quarantine has ended.

Another seriously worrying trend identified in the examples is how **biometric mass surveillance technologies are being deployed disproportionately against certain groups.**

In Germany, religious and LGBT+ communities have been the targets of live facial recognition.

In the Netherlands, foreign nationals have been included in pseudo-criminal biometric databases purely for the reason of being an "alien, and the dystopian 'Living Labs' project has seen **whole communities used as experiments,** often without their knowledge, in which their biometric data are pooled with other data to try and predict their levels of aggression or their life outcomes (e.g. education) **within a welfare and social system already known to punish and criminalise poor or working-class people and people of colour.**

**Whilst there have been many notable successes in stopping rights-violating uses of biometric surveillance in Europe since the release of "Ban Biometric Mass Surveillance", the problem continues to accelerate, showing exactly why EDRi's call is more important than ever.** As the researchers summarise:

**"The use of biometric mass surveillance in public spaces has increasingly, and quietly, become regular practice in recent years."**

Since October 2020, a civil society campaign led by EDRi, **called Reclaim Your Face, has risen up to contest the issue,** despite claims from the European Commission that current rules and measures suffice.

To the contrary, **this research further demonstrates the lacuna between a true ban – in which such harmful and rights-violating uses could not be deployed in the first place – and today's biometric mass surveillance Wild West,** where private companies, profit, and the state impulse to monitor, surveil, and control people at all times prevail.

*Foreword written by EDRi*

# INTRODUCTION TO GERMANY COUNTRY STUDY FROM EDRI:

**The first case study in this report focuses on Germany, a country often spoken about as a shorthand for high standards of privacy and data protection. Yet the research reveals the systematic biometric mass surveillance practices that are proliferating by both public and private actors (and often in collusion with one another) across Germany.**

It shows worrying trends of biometric surveillance deployments shrouded in secrecy, exacerbating structural discrimination, and posing serious threats to people's dignity. It shows civil society and concerned citizens shouldering the burden of fighting for our rights. And it paints a picture of towns and cities where convenience and efficiency are overtaking the law – at the detriment of people's human rights.

As this case study shows, people on German streets, in shopping centers, at religious venues, and in commuter stations have all been subject to invasive biometric mass surveillance.

The notorious company Clearview AI have been proven to be acting illegally with the data of German citizens, but Clearview AI have avoided fines and have not been ordered to stop their unlawful practices by German authorities. Ever-growing biometric identity databases run by the state have called into question whether Germans are being given a true chance to consent to giving their biometric data as required under EU law.

And issues such as online age verification and contactless biometric identification in light of COVID-19 are posing risks to people's rights that may extend far beyond when the health emergency is over.

This research charts how, for almost 20 years, digital surveillance infrastructures across Germany have been quietly growing. The evidence shows that in recent years, facial recognition algorithms have increasingly been retrospectively – and unlawfully – applied to collected footage.

There has been a rise in supposedly standard CCTV cameras being sold with in-built biometric analysis capabilities, without care for whether this practice is lawful in the jurisdiction and context in which it is being sold. In just one example, the company Dallmeier has sold these biometric-ready cameras to police in 19 different German cities.

They offer the potential to infer if people are jaywalking or loitering – exceptionally petty crimes which cannot and should not justify the use of such invasive technologies.

In another example, since 2018, so-called "biometric ready" cameras have been installed in the city of Cologne, surveilling areas that contain GP practices, law firms, places of worship, and LGBT+ venues.

Given that EU and national laws require personal data processing to always be necessary and proportionate to the specific circumstance, the fact that the police would install biometric mass surveillance devices without any specific purpose, covering areas where people could easily be associated to their protected characteristics (e.g. their religion or sexuality) and therefore with high risks of discrimination – simply for the purpose of "just in case" - is not only chilling, but flouts the principles of data protection and fundamental rights.

In 2021, the Cologne Administrative Court stepped in to stop the use of these devices, but a final decision is pending – and shows the dangers of the European regime that fails to prevent such uses from being deployed in the first place.

These are some of the many reasons why the EDRi network has argued that existing 'in-principle' prohibitions and limitations on biometric processing are not sufficient to protect people's rights and freedoms. Existing laws have not translated into a real ban – and EU-wide action is needed to sufficiently ban biometric mass surveillance practices.

# GERMANY

**While the right to privacy and informational self-determination is not expressly enshrined in the German constitution, such a right was held as lying impliedly within Article 2, paragraph 1 (the protection of personal freedom) and Article 1, paragraph 1 (the protection of human dignity) by the Federal Constitutional Court in Mikrozensus.** [2]

It is also important to note that Germany is a signatory to three legal instruments incorporating a right to privacy – the Universal Declaration of Human Rights, The European Convention on Human Rights, and the International Covenant on Civil and Political Rights. Germany has also been often recognised for having a strong privacy culture.

A recent survey by the Vodafone Institute highlights that Germans are particularly skeptical of 'Big Data' and are acutely sensitive about how their personal data is used, with only 19% of German participants strongly trusting the state with their personal data.[3] Germany has also integrated the GDPR into domestic law through its federal data protection act ('BDSG').

Despite its privacy culture and legal engagement with privacy rights, instances of biometric mass surveillance can be identified in Germany. This section explores a growing trend of public and private actors implementing practices capable of being considered biometric mass surveillance.

Our research suggests that this is often done in a manner which lacks adequate transparency, with concerns being raised as to whether such technology is necessary and proportionate for its purported purposes.

This section focuses on four key types of biometric deployment in Germany:

**1.** Facial recognition in public spaces;
**2.** Fingerprint requirements on national identity cards;
**3.** Online age and identity 'verification';
and COVID-19 responses. These will be discussed in turn.

---

[2] **BVerfG, Urteil des Ersten Senats vom 15 Dezember 1983 – 1 BvR 209/83, available at** https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html

[3] **Vodafone Institute for Society and Communications, 'Big Data: A European Survey on the Opportunities and Risks of Data Analytics' (Vodafone, 2016) available at** https://www.vodafone-institut.de/bigdata/links/VodafoneInstitute-Survey-BigData-Highlights-en.pdf

# 1. FACIAL RECOGNITION

## 1.1 Local Government

Reliance by law enforcement agencies on mass/general facial recognition practices varies across Germany due to the relatively high autonomy exercised by the federal states and their constituent local authorities. However, we have identified an increasing trend of implementation of such biometric surveillance measures across numerous localities throughout Germany.

The infrastructure required to facilitate facial recognition in public spaces has been gradually developed over the past two decades. In 2003 state authorities in North Rhine-Westphalia ('NRW') began implementing pilot surveillance regimes in Bielefeld and Coesfeld.[4]

Subsequently, similar surveillance regimes began emerging in Mönchengladbach in 2004[5] and Düsseldorf in 2009.[6] As at November 2020, approximately 79 stationary cameras of the NRW state police are currently in operation in the public space of central Cologne.[7]

Further examples include Aachen, where a pilot surveillance programme from 2008 was reimplemented in 2017,[8] and Bonn, where police have been introducing video surveillance based on mobile camera setups as of September 2020.[9]

Once the images collected by video surveillance are subject to biometric processing, either live during capture or at a later point (for example in 1.1.1), this would constitute mass biometric surveillance.

To illustrate the scale of privacy intrusions that these "pilot programs" can encompass, during the G20 Summit in 2018, the Hamburg DPA found that Hamburg's police force had collected c. 17 terabytes worth of images and videos which were processed through automated facial recognition technology.[10] Concerningly, the Hamburg DPA identified that this had been done without a legal basis.[11]

---

4 **Markus Lang: Die Evaluation der Videoüberwachung in Bielefeld. Zugleich eine Erwiderung zu Quambusch.** In: Kriminalistik. 2005, S. 723–726.

5 **'Hier gibt es Videoüberwachung in Mönchengladbach' (RP Online) available at** https://rp-online.de/nrw/staedte/moenchengladbach/hier-gibt-es-videoueberwachung-in-moenchengladbach_bid-9124669

6 **Siedentop, C., 'Nach Gewalttat in Mönchengladbach: Bessere Videoüberwachung soll Bürger schützen' (RP ONLINE 2012) Available at:** https://rp-online.de/nrw/panorama/bessere-videoueberwachung-soll-buerger-schuetzen_aid-13675387

7 **'Stand der Videoüberwachungsorte in Köln' (Kameras stoppen, 2020) Available at:** https://kameras-stoppen.org/videobeobachtung-in-koeln

### 1.1.1 Case Study – Cologne

Cologne is a particularly salient case study of the use of mass surveillance technology on the part of local authorities and law enforcement in Germany.

In terms of infrastructure, the Cologne Police Headquarters has deployed 26 additional stationary video cameras into operation on the main station forecourt and around the Cologne Cathedral since April 2016. The cameras used by Cologne are high-end 'biometric-ready' cameras, i.e., they are capable of live facial recognition.[12]

This area, together with the Breslauer Platz behind the main station, presents itself as a high level surveillance network covering an area of approx. 300,000 to 360,000 square meters.
Prior to the installation of the biometric ready video cameras, available statistical data evidenced that crime was declining in the area. However, notwithstanding the downward trend of crime, the use of video surveillance is increasing.[13] Appendices 1 and 2 enclose a mapped overview of the scope of the surveillance regime that has so far been implemented by Cologne Police.

The Cologne case study also illustrates the increasing threat of privacy violations by law enforcement agencies, as a wide array of citizens and businesses conducting lawful activities are within scope of Cologne's surveillance regime.

For example, in addition to pedestrians, cyclists, cars (including license plates, which are not pixelated), GP practices, pharmacies, law firms, and places of worship are all in view of this surveillance.

These areas include Rudolf Platz,[14] which hosts a number of LGBT+ venues, and other areas, including Breslauer Platz, which host places of worship.[15]

---

8 **Straßenkriminalität: Polizei in NRW setzt häufiger auf Videoüberwachung (DIE WELT, 2021) Available at:** https://www.welt.de/regionales/nrw/article206038077/Strassenkriminalitaet-Polizei-in-NRW-setzt-haeufiger-auf-Videoueberwachung.html 'Videoüberwachung in Aachen und Düren ab 2008' (Aachener Nachrichten, 2007) Available at: https://www.aachener-nachrichten.de/nrw-region/videoueberwachung-in-aachen-und-dueren-ab-2008_aid-27935235

9 **Leurs, T., 'Überwachung in Bonn: Polizei nimmt Videokameras am Rheinufer in Betrieb' (General-Anzeiger Bonn 2020). Available at:** https://ga.de/bonn/stadt-bonn/videoueberwachung-am-rheinufer-bonn-polizei-nimmt-kameras-in-betrieb_aid-53147327

10 **Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ('HmbBfDI'), 'Pressemitteilung: Einführung der automatisierten Gesichtserkennung beanstandet' (2018) Available at:** https://datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360

11 **HmbBfDI, Einsatz der Gesichtserkennungssoftware „Videmo 360" durch die Polizei Hamburg zur Aufklärung von Straftaten im Zusammenhang mit dem in Hamburg stattgefundenen G20- Gipfel. (Hamburg, 2018). Available at:** https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

12 **The cameras are most likely supplied by the biometrics firm Dallmeier, which has publicly stated collaboration with several German state authorities, including Cologne.** See section 1.3.2 below.

The collection of data that may tie individuals to such venues and services may reveal further aspects of their private life, such as sexual orientation or religious belief, which are given further protection alongside biometric data under Art. 9(1) GDPR, and raises further questions of discriminatory impacts that biometric mass surveillance has on minoritised groups.

In a decision of 18 January 2021, the Cologne Administrative Court issued an injunctive order against the Cologne Police to immediately stop video surveillance of Breslauer Platz and its side streets in Cologne.[16] The injunction remains extant until a final decision in the main proceedings, which remain ongoing.[17] The final decision of the Cologne Administrative Court awaits to be seen.

The reasoning of the Cologne Administrative Court classified the crime rate in Breslauer Platz as low in absolute terms.[18] The Court considered the video surveillance to be unreasonable in its interference with the plaintiff's fundamental right to informational self-determination.[19] However, the Court reasoned that the ongoing risk of being surveilled and identified during the COVID-19 lockdown are relatively low due to the requirement to wear a mask.[20]

In light of facial recognition software recently being developed to work on mask-wearers, this may not have been as effective as the Court may have understood it to be.[21]

According to Cologne police headquarters, the 14-day storage period for all video recordings should serve to preserve evidence in the instance that crimes in those locations are reported.

However, in 2017 in the monitored area of the cathedral and main station (already equipped with at least 25 video cameras) just 85 such archiving processes were carried out to preserve evidence.[22] This indicates that, of the thousands of individuals subjected to surveillance in the relevant areas, less than 0.1% of what was recorded was considered to have probative value, questioning the proportionality of a measure which surveils all passers-by.

---

13 **Verwaltungsgericht Köln, (18 January 2021) Az.: 20 L 2340/19, available at** http://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2021/20_L_2340_19_Beschluss_20210118.html ('20 L 2340/19') para 46.

14 **See appendix** 2.

15 **E.g. the St. Lupus parish, located just across the southern camera in appendix** 1.

16 **20 L 2340/19 supra** (n 12).

17 **'Videoüberwachung Breslauer Platz gestoppt' (Kameras stoppen, 2021) Available at:** https://kameras-stoppen.org/videoueberwachung-breslauer-platz-gestoppt

18 **20 L 2340/19 supra (n 12) para.** 47.

19 **ibid, para.** 55.

20 **Ibid, para** 38.

21 **See section** 4 **below.**

22 **'Klage gegen die Videoüberwachung in Köln' (Kameras Stoppen, 2021)** https://kameras-stoppen.org/klage-videobeobachtung-koeln

## 1.2 Federal Government

Germany's federal government has been exploring the uses of mass biometric surveillance in recent years, primarily in respect of installation on public transport. The mission of Germany's federal police includes providing transportation security at German railway stations[23] and international airports.[24]

In 2017, federal authorities announced a trial project to test facial recognition surveillance technology at Berlin's widely-used Südkreuz train station.[25] It was to include trials of live video analytics including behavioural analysis for security purposes – although Deutsche Bahn, Germany's largest railway company whose sole shareholder is the Federal Republic of Germany,[26] has been mentioned to also have an interest in preventing graffiti tags on its trains.[27]

The project was met with resistance by civil society actors and activists who argued that the technology used is more extensive than its proponents admit.[28]

In December 2020, the federal government and Deutsche Bahn announced an increase in security measures at train stations, primarily through increasing the amount of deployed cameras by c. 3,000.[29]

The announcement included reference to an increase in the overall technical capabilities of the cameras to be deployed, including higher resolution imagery and reference to "intelligent video analysis" in certain locations, strongly implying the use of biometric processing given the purported security interests in identifying individuals.

The only reference to arguments against such deployments concern impacts on train punctuality and passenger capacity – but no mention of surveillance concerns or fundamental human rights, including the right to privacy.

---

23 **Bundespolizeigesetz 1994 ('BPolG')** s3.

24 **BPolG,** s4.

25 **'Sicherheitsbahnhof Berlin Südkreuz' (Bundesministerium des Innern, für Bau und Heimat 2017)** https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html

26 **'DB-Konzern - Facts & Figures' (Web.archive.org)** https://web.archive.org/web/20090426010642/http://www.deutschebahn.com/site/bahn/en/db__group/corporate__group/ata__glance/facts__figures/facts__figures.html

27 **Koschyk, M., 'Big brother in Berlin: Face recognition technology gets tested' (Deutsche Welle, 31 July 2017) available at** https://www.dw.com/en/big-brother-in-berlin-face-recognition-technology-gets-tested/a-39912905

## 1.3 Biometric Technology Providers in Germany

Biometric mass surveillance technology is a lucrative market involving public and private organisations around the world and is expanding exponentially. The technical capacity to implement live biometric mass surveillance through facial recognition technology depends on various factors, but the following two components are essential: **(1)** hardware capable of biometric processing; and **(2)** software that facilitates biometric processing of captured images.

### 1.3.1 Hardware

Increasingly, the cameras used to implement surveillance regimes that utilise facial recognition technology are outfitted with features that enable live video analytics.

These cameras constitute a growing subset of CCTV cameras that are internet protocol (IP) cameras, which use local area networks (LANs) to transmit video across networks in real time.[30]

Modern cameras, as opposed to the previous analogue CCTV models, utilise a combination of higher resolution image capture, inbuilt processors to assist with live analytics, and the ability to connect to local networks and databases across regions and even countries and continents in real time.[31]

Such cameras are effectively "biometric-ready", the capacity for biometric surveillance being a design feature from the start. That is, the technology is intentionally designed by their creators to have the capability for biometric data collection, regardless of whether such data-collection and or surveillance technology, or use of it, is legal/lawful in the jurisdictions in which it is intended on being sold.

Biometric-ready cameras have already been utilised by German law enforcement authorities for surveillance purposes.

One example of a private corporate partner of police surveillance throughout Germany is a company called Dallmeier. In April 2020, Dallmeier issued a statement stating that its camera systems and relevant software are being deployed by German police in at least 19 cities in Germany.[32]

These cities include larger cities such as Cologne, Frankfurt, Essen, Wiesbaden, and Bremen. The statement also cites Thorsten Wünschmann, head of the Public Order

Office in the city of Hanau, as saying that "[The Public Order Office] has been using the Dallmeier Panomera technology since 2018 with great success."[33] The cameras in the Panomera range are multifocal and allow for multiple users to access streams at the same time.[34] They have extensive and accurate zoom capacity and, as they have inbuilt processors, are capable of live biometric processing.[35]

Dallmeier is far from the only provider of cameras capable of live video analytics – another example is the company Cognitec,[36] whose operations are described in more detail below.[37]

Such collaborations between state authorities and private biometrics firms raise legal, ethical, and regulatory issues which warrant emphasis.

Firstly, the normalisation of biometric mass surveillance in public spaces is legitimised through the contractual arrangements between public and private actors. Private actors have an innate incentive to maximise profits, which may further spur the use of biometric mass surveillance tools.

Secondly, private corporate actors marketing so-called "solutions" in response an increasing range of behaviours (e.g., loitering, jaywalking, etc.[38]) raises further questions of proportionality that will be examined below.[39]

---

28 **'Germany's Facial Recognition Pilot Program Divides Public' (Deutsche Welle, 2017)** https://www.dw.com/en/germanys-facial-recognition-pilot-program-divides-public/a-40228816

29 **Bundesministerium des Innern, für Bau und Heimat, 'Bundesregierung Und Deutsche Bahn Beschließen Weitere Maßnahmen Für Mehr Sicherheit An Bahnhöfen' (2020)** https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/sicherheit-bahnhoefe.html

30 **Cheng, J., 'Securing IP Surveillance Cameras in the IoT Ecosystem' (Trend Micro, 18 April 2018) available at** https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/securing-ip-surveillance-cameras-in-the-iot-ecosystem

31 **Sadun, Erica Digital Video Essentials: Shoot, Transfer, Edit, Share (26 December 2006)** ISBN 9780470113196.

32 **Dallmeier, 'Dallmeier Presents Success Record For Video Security In The German "Safe City" Segment' (2020)** https://www.dallmeier.com/index.php?id=384

33 **Ibid.**

34 **'Panomera® Cameras' (Dallmeier electronic)** https://www.dallmeier.com/technology/panomera-cameras (See "Multi-user and multicast")

35 **Ibid.**

36 **'Facevacs-Videoscan' (Cognitec)** https://www.cognitec.com/facevacs-videoscan.html

37 **See Section** 1.3.2.

38 **Panomera S Series Brochure (Dallmeier)** https://www.dallmeier.com/fileadmin/user_upload/PDFs/Technology/Panomera/Dallmeier_Panomera_S-Series_Brochure_EN.pdf

39 **See section** 1.4.5.3.

### 1.3.2 Software

In addition to the technical capacities for biometric mass surveillance of camera technology, there are a number of private companies working with both German law enforcement authorities and privately owned stadiums/shopping centres that offer software capable of biometric processing. For example:

#### Cognitec

Cognitec is a facial recognition software company based in Dresden. It publicly lists partnerships with the German Federal Criminal Police (BKA) and Federal Office of Administration.[40] Its principal law-enforcement software, 'FaceVACS-DBScan LE', advertises the capacity to compare faces to local or central multi-million image databases.[41]

It also offers the ability to search through media sets according to a variety of criteria which include "all persons" seen during a specific time frame or location.[42]

Cognitec offers products for both public and private use, such as its FaceVACS-Videoscan.[43] Its applications are advertised to include surveillance of both public and privatised (but publicly-accessible) spaces including shopping malls, banks, airports, and hospitals.[44]

The marketing used in a flyer for the software is a good illustration of the purported scope of Cognitec's surveillance service.[45] It advertises being able to answer questions about personal relations between people, such as when two people were last seen together.[46] This software offers both individual and crowd analytics.

This indicates that the market for biometric mass surveillance tools also responds to demand from other private actors who operate spaces accessible to the public. As private actors are subject to fewer transparency obligations than public authorities, the exact extent to which they deploy biometric mass surveillance is difficult to pinpoint.

However, the prevalence of software products marketed for private use (despite the fact that they are deployed in publicly-accessible spaces) indicates that enough of a demand exists to establish a prevalent practice in Germany and Europe more broadly.

#### Clearview AI

The extent of the controversial US-based Clearview AI Inc.'s involvement in the EU has been difficult to assess. Clearview AI scrapes photos from the internet to create a database of searchable biometric profiles, giving it relevance insofar as it applies in the EU.

Further research appears to suggest that Clearview AI has been engaged in a campaign of evasion, obfuscation, and misinformation about its operations in the EU, paired with delayed responses by public authorities.

We note the following series of requests and correspondences as evidence of this.

In January 2020, a Hamburg resident submitted a data subject access request to Clearview AI, which required him to send a photo of his face.[47] Clearview AI in response issued a request for a government issued ID, which the resident refused.

In a partial response, Clearview AI sent search results based on the provided photo, along with confirmation that the resident's photo had been deleted in February 2020.

The resident then submitted a complaint to the Hamburg DPA, on the basis of Clearview AI processing his biometric data without his consent, as well as impugning the incomplete response of Clearview AI to his requests.

The complaint was first rejected on 5 March 2020, as the DPA claimed that the GDPR was not applicable as Clearview AI was not considered to be used in the EU.[48]

Following further submissions by the resident and support from civil society actor Noyb,[49] the Hamburg DPA launched an investigation into the matter.[50]

During this period in March 2020, Clearview AI declined to answer questions about processing.[51] By May 2020, Clearview AI had sent the resident an unsolicited response which revealed that it did not in fact delete the resident's photo, and its answer contained not only further images of the resident but also those of eight other people. By August, the DPA ordered Clearview AI to answer a questionnaire under threat of penalties,[52] to which Clearview AI responded in September 2020.

By January 2021, the Hamburg DPA launched administrative proceedings against Clearview AI, ordering the deletion of the mathematical hash value representing the resident's profile, as well as ordering confirmation that Clearview AI had done so.[53] It should be noted that this was a partial order limited to a specific claimant, but the DPA's reasoning establishes four key developments, as follows:

**1.** Firstly, it confirmed Clearview AI was being used and expanded in the EU.

**2.** Secondly, it characterises Clearview AI's activities as monitoring, despite Clearview AI's claims to the contrary. Clearview AI did not simply create a snapshot of some photos in a vacuum, but rather collected biometric data over a period of time as new images would be created or discovered. It also not only collected images, but also archived their sources and associated data. This, according to the DPA, constituted monitoring.[54]

**3.** Thirdly, it establishes that Clearview AI's operations fell within the scope of the GDPR. This implies that any monitoring and biometric processing that Clearview AI applies to EU citizens is judiciable by European DPAs and similar authorities. The resident here was not the only European citizen monitored by Clearview AI, nor will they be the last.

**4.** Fourthly, it found that Clearview AI processed the resident's biometric data without a legal basis.[55] It also emphasised that there was no consent on the part of the data subject.[56] Therefore, the processing of the biometric data of other European data subjects by Clearview AI equally lacks the requirements of legality and consent.

---

40 **'Partners' (Cognitec, 2020)** https://www.cognitec.com/partners.html

41 **'Facevacs-Dbscan LE - Cognitec' (Cognitec)** https://www.cognitec.com/facevacs-dbscan-le.html

42 **'FaceVACS-DVScan LE flyer', (Cognitec)** https://www.cognitec.com/facevacs-dbscan-le.html

43 **'FaceVACS-Videoscan' (Cognitec.com)** https://www.cognitec.com/facevacs-videoscan.html

44 **'FaceVACS-VideoScan flyer' (Cognitec).** https://www.cognitec.com/facevacs-dbscan-le.html

45 **Ibid.**

46 **Ibid.**

47 **'Clearview AI In Der EU Illegal, Aber Nur Begrenze Löschungsanordnung' (noyb, 2021)** https://noyb.eu/de/clearview-ai-der-eu-illegal

48 **'Clearview AI In Der EU Illegal, Aber Nur Begrenze Löschungsanordnung' (noyb.eu, 2021)** https://noyb.eu/de/clearview-ai-der-eu-illegal

49 **Ibid.**

50 **Beuth P, 'Hamburgs Datenschützer Leitet Prüfverfahren Gegen Clearview Ein' (Spiegel.de, 2020)** https://www.spiegel.de/netzwelt/web/clearview-hamburgs-datenschuetzer-leitet-pruefverfahren-ein-a-0ec1870d-c2a5-4ea1-807b-ac5c385ae165

51 **HmbBfDI, ' Anfrage #195578: Fragenkatalog An Clearview AI' (2020) available at** https://fragdenstaat.de/anfrage/fragenkatalog-an-clearview

52 **Ibid, attached document available at:** https://fragdenstaat.de/anfrage/fragenkatalog-an-clearview/516080/anhang/BescheidmitFragenkatalog.pdf

53 **HmbBfDI, 'Consultation Prior To An Order Pursuant To Article 58(2)(G) GDPR' (2021) available at** https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.PDF

54 **Ibid,** p 2.

55 **Ibid,** page 3.

56 **Ibid.**

The findings of the Hamburg DPA indicate a deep and intrusive practice of biometric surveillance in the EU by foreign actors.

Although the DPA's decision against Clearview AI was noteworthy in its findings, it did not go as far as to evaluate the broader implications nor adjudicate on the matter further.

It is also worth noting that the proceedings took almost a year to reach the remedial stage and have been greatly characterised by the burden falling predominantly on the shoulders of concerned citizens and civil society to keep proceedings afloat and raise FOIs in response to opaque processes and the lack of enforced checks.

### Dallmeier

Dallmeier also provides authorities with software. 'HEMISPHERE' is its principle analytic technology and is present in its live-analysis capable cameras.[57] HEMISPHERE is advertised to capture a wide variety of data fully automatically.[58] It can be programmed to observe various behaviours, such as loitering, parking, intruding, vehicle counting, and crowd analysis.[59]

'HEMISPHERE' is accompanied by two other relevant biometric processing software products: SMAVIA and AnyVision. SMAVIA is a software capable of biometric processing, applying to data that was not subject to biometric processing at the time it was gathered – it is effectively capable of retrospective processing.[60] AnyVision is Dallmeier's facial recognition software which is already available in Dallmeier's systems.[61] The exact extent to which HEMISPHERE is currently being applied to biometric mass surveillance is unclear.

### Videmo

Since 2018, the police in Hamburg used the facial recognition software "Videmo 360"[62] developed by biometrics firm Videmo to investigate incidents connected to the G20 summit in 2018.[63]

Videmo 360 was used to identify persons by processing images from private recordings, police video surveillance, and recordings from train station CCTV with the use of public and private databases. This information was then kept on a police database.

The Hamburg DPA issued proceedings against the Hamburg police, ordering them to delete this database, arguing that the police did not have sufficient authority for biometric processing that could justify an intrusion on fundamental rights.[64]

The Hamburg Administrative Court reversed this decision on principally procedural grounds, primarily arguing that the DPA lacked the competence to conduct the review and the relevant legal basis for doing so.[65]

A salient part of the judgement concerned the construction of the test which applies to the processing of special categories of data under federal data protection law, as the constituent element of "strict necessity" was instead read as to mean "tactically sensible".[66]

This appears to be a statement of a reasonableness test at law. Hamburg DPA has since appealed the decision,[67] as this presents a key area of legal development in regard to Germany's approach to biometric mass surveillance more broadly. The appeal is still waiting to be heard.

In the meantime, following the judgement of the Hamburg Administrative Court, the Hamburg police have continued to use Videmo 360 for mass biometric surveillance in Hamburg, but have publicly confirmed that they recently deleted the G20 database.[68]

Although Hamburg's police authorities have argued that the matter was no longer justiciable, the Hamburg DPA rejected this argument and stated that, due to the practice being ongoing and due to the relevance of the proceedings to the DPA's continued work in future, the appeal should be allowed. [69]

In a press release from 28 May 2020, the Hamburg DPA stated that although the recent deletion of the biometric G20 database by the Hamburg police was welcome, questions remain in regards to where the line will be drawn relating to the controversies surrounding the use of Videmo 360 and other such biometric mass surveillance tools.[70] The statement also highlighted the "considerable dangers" automated face recognition poses to a free and democratic society, and the Hamburg DPA called for more extensive judicial clarification on the matter.[71]

---

57 **Software (Dallmeier) available at** https://www.dallmeier.com/technology/software

58 **Ibid.**

59 **Ibid.**

60 **'Dallmeier Releases New Tutorial Videos On Viewing Software Smavia Viewing Client' (Sourcesecurity)** https://www.sourcesecurity.com/dallmeier-smavia-viewing-client-cctv-software-technical-details.html

61 **Dallmeier integrates AnyVision facial recognition into its "HEMISPHERE®" software platform for security and business (Dallmeier.com) available at:** https://www.dallmeier.com/about-us/press-centre/anyvision-facial-recognition#c1219

62 **'Videmo 360' (Videmo) available at** https://videmo.de/en/products/videmo-360

63 **'G20-Krawalle: Polizei Ignoriert Löschanordnung Des Datenschützers' (Heise, 2021)** https://www.heise.de/newsticker/meldung/G20-Krawalle-Polizei-ignoriert-Loeschanordnung-des-Datenschuetzers-4537317.html?wt_mc=rss.ho.beitrag.rss

64 **HmbBfDI, 'Az.: 11.03-13 - Einsatz Der Gesichtserkennungssoftware „Videmo 360" Durch Die Polizei Hamburg Zur Aufklärung Von Straftaten Im Zusammenhang Mit Dem In Hamburg Stattgefundenen G20-Gipfel'(2021)available at** https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

65 **Verwaltungsgericht Hamburg, (Hamburg Administrative Court 2019) Urteil vom 23 Oktober 2019 Az. 17 K 203/19 available at** https://justiz.hamburg.de/contentblob/13535554/cc5a1e8c70c95088220147f57921d22d/data/17-k-203-19.pdf

The current appeal by the Hamburg DPA itself is noteworthy on two key issues. Firstly, it highlights that much of the domestic law does not have a clear answer for how facial recognition software, as well as biometric mass surveillance more generally, finds a clear basis in domestic law.

Secondly, it highlights concerns on the part of DPAs in respect of the "broad encroachment" on fundamental rights risked by the use of biometric mass surveillance.

## IDEMIA

The German Federal Criminal Police Office (BKA) is also considering replacing its face recognition from Cognitec with an application from IDEMIA.[72] As part of the Berlin Südkreuz pilot project, the Federal Police, BKA, and Deutsche Bahn tested a face recognition system from IDEMIA in addition to two other products.[73] The software was also tested in the German security research project FLORIDA.

IDEMIA, formerly known as OT-Morpho, courted controversy in Kenya during the contested 2017 election when it was forced to deny claims that its biometric voter identification system had been hacked.[74]

Opposition leaders have accused the company, which supplied voter identification and results transmission kits, of misconduct — an allegation that IDEMIA has denied.[75]

A recent report[76] by Privacy International and the Centre for Intellectual Property and Information Technology Law (CIPIT) has shown that voter data was available for sale in the run-up to the election.[77]

The Kenyan Parliament voted to ban IDEMIA from conducting business in the country for at least ten years.[78]

---

66 **Ibid p** 21.

67 **HmbBfDI, 'Antrag auf Zulassung der Berufung §§ 124, 124a VwGO Az. 5 Bf 46/20.Z - Begründung des Antrags vom 6.2.2020' (to Hamburg Administrative Appeal Court 2020) available at** https://datenschutz-hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf

68 **HmbBfDI, 'Polizei Hamburg Löscht Die Im Zuge Der G20-Ermittlungen Erstellte Biometrische Datenbank Zum Gesichtsabgleich' (2020) available at** https://datenschutz-hamburg.de/pressemitteilungen/2020/05/2020-05-28-datenbank-loeschung ('HmbBfDI Press Release 2020').

69 **HmbBfDI, 'Stellungnahme Des Hmbbfdi Vom 20. Juli 2020 Zur Zulässigkeit Der Berufung Az.: J / 11.03-13' (2020) available at** https://datenschutz-hamburg.de/assets/pdf/Stellungnahme_Zulassung_Berufung_2020-07-20.pdf

70 **See supra** (n 65).

71 **Ibid**.

72 **Monroy, M., 'Projekt Interoperabilität: EU zahlt 300 Millionen Euro für Erkennung von Gesichtern und Fingerabdrücken' (Netzpolitik, 2020). Available at:** https://netzpolitik.org/2020/eu-zahlt-300-millionen-euro-fuer-erkennung-von-gesichtern-und-fingerabdruecken

73 **Ibid**.

74 **'French firm OT-Morpho says IEBC voting system was not hacked' (TechTrendsKE, 2017)** https://techtrendske.co.ke/french-firm-ot-morpho-says-iebc

## 1.4 Legal Analysis

Our examination of the issues raised by mass facial recognition in public spaces will be evaluated in two stages. Relevant laws and principles from German, European, and International law will be identified and analysed in light of the above findings.

The issue of 'biometric-ready' cameras will also be assessed in terms of the right to dignity, structural discrimination, and proportionality.

### 1.4.1 German Law

Germany's Federal Constitution enshrines the universal human rights recognised under the UDHR. The power to establish video surveillance (including biometric ready video surveillance) of publicly accessible spaces is enshrined both in German federal law as well as the law of various federal states.[79]

At the federal level, section 4 of the Federal Data Protection Act ('BDSG') allows for video surveillance of publicly accessible areas only as far as is necessary.[80]

The BDSG however does not apply in some instances where federal states and local authorities have their own provisions for surveillance of public spaces. Bavaria[81] and NRW[82] have special provisions for surveillance in public spaces.

#### 1.4.1.1 Scope

The BDSG prescribes three grounds under which such surveillance can be established: for public bodies to perform their tasks; to exercise the right to decide who is permitted to access a certain area or service; and to safeguard legitimate interests for specifically defined purposes.[83]

---

75 **'OT-Morpho denies claims Kenyan biometric voting system was hacked' (BiometricUpdate, 2017)** https://www.biometricupdate.com/201709/ot-morpho-denies-claims-kenyan-biometric-voting-system-was-hacked

76 **Strathmore University Centre for Intellectual Property and Information Technology Law 'Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process (2018) available at** https://www.cipit.strathmore.edu/wp-content/uploads/2018/05/Biometrics-Privacy-Report-by-CIPIT.pdf

77 **Ibid.**

78 **'For credible elections, MPs vote to block Huduma Namba firm' (Nation, 2019) available at** https://nation.africa/kenya/news/for-credible-elections-mps-vote-to-block-huduma-namba-firm-161510

79 E.g. Bavaria and NRW, notes 77 and 79 respectively.

80 **Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626) ('BDSG'),** Section 4(1).

81 **Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei** (Polizeiaufgabengesetz – PAG) 1990, s33.

82 **Polizeigesetz des Landes Nordrhein-Westfalen** (PolG NRW) s15a.

It is worth noting that the third ground is open-ended and renders the grounds functionally non-exhaustive. In the absence of 'legitimate overriding interests' of data subjects, video surveillance of large publicly accessible facilities, e.g., arenas and shopping centres, or for vehicle parking and public transport is generally permitted.[84]

In terms of the processing of biometric data, sections 22 and 48 BDSG refer to the special categories of data under Article 9(1) GDPR, which includes biometric data.

Section 48 BDSG also includes a test of "strict necessity" for the processing of special categories of data. In respect of both private and public bodies, the BDSG permits the processing of biometric data if necessary for rights related to social security and related obligations[85] or medical purposes,[86] necessary for reasons in the area of public health,[87] or *urgently* necessary for reasons of substantial public interest.[88]

For public bodies only, further exemptions are outlined where processing is necessary to prevent a substantial threat to public security,[89] *urgently* necessary to prevent "substantial harm to the common good"[90] or necessary for urgent reasons of defence or intragovernmental obligations.[91]

This establishes a very high bar for necessity in respect of the processing of biometric data by public authorities, characterised by urgency and the substance of identifiable threats.

At the state level, the provisions in Bavaria and NRW also require an assessment of necessity based on the likelihood of crimes being committed in the relevant areas.[92] However, these reference only the recording of images or audio and do not explicitly address biometrics, which is principally governed by s48 BDSG.

Specifically, as regards the federal police, the federal police act (BPolG) outlines instances in which federal police can conduct surveillance in public spaces and identify individuals.

Federal police are permitted to collect personal data in the context of public events or gatherings *if facts justify* the assumption that during or in connection to an event or gathering considerable dangers to security exist.[93] Other provisions regarding the identification of a natural person concern individual identification on the basis that they have or are about to commit a crime.[94] In effect, the act principally only sanctions identification in limited circumstances and must equally be justified under a strict test of necessity - responding to an immediate and identifiable risk.

The strict necessity test must also be viewed in light of the countervailing fundamental rights concerns. According to Germany's Federal Constitutional Court (BVerfG), interferences on fundamental rights are particularly intrusive if they are hidden and broad in scope, i.e., where numerous people are included who are unrelated to a specific misconduct and did not cause the interference with their own behaviour.[95]

#### 1.4.1.2 Necessity

With Cologne and at least 18 other German cities using biometric surveillance tools in public spaces,[96] the grounds on which this is justified warrants further scrutiny. Such surveillance has now been operating for several years, depending on location, and generally takes the form of precautionary measures that seek to provide law enforcement with general supervision.

Although the domestic legislation requires the processing of biometric data to be tailored to substantive and/or urgent threats to public security, biometric mass surveillance appears to have been deployed in a general manner in the hope that something of interest may be discovered. This is difficult to align with the highly set bar for necessity outlined in the legislation.

At the federal level, it is difficult to ascertain the full scope of biometric surveillance at train stations and airports as federal police do not record the frequency or duration of their surveillance.[97]

However, the framing of the legislation paired with the prolonged use of biometric mass surveillance adds to proportionality concerns as it is, by nature, a covert means of affecting an unprecedented number of people.

At the state level, the findings of the Cologne Administrative Court have indicated that mass surveillance, including biometric mass surveillance, has continued in places where crime rates have not been increasing, further undermining the purported necessity of such practices by state authorities.

Both federal and state authorities appear to operate on the assumption that biometric mass surveillance is inherently justified where a general crime rate exists.

This is difficult to reconcile with the high statutory test that applies to the processing of special categories of data under BDSG s22(1)(2)(1), in that if regular or petty crime rates can constitute a "substantial threat to public security" then it is unclear where the line can be drawn at all.

In terms of private actors, there is also the matter of an increased reliance on biometric mass surveillance in respect of petty crimes and non-criminal behaviour.

From private biometrics firms advertising services that can detect loitering or "valued customers" to private bodies having potential interest in using biometrics to detect graffiti or petty theft, the scope of what biometric mass surveillance is being used for is expanding.

Although the uses for the deployment of biometric mass surveillance have increased in accordance with this trend, the intrusiveness of the mass collection and processing of biometric data remains the same. This is a particular concern regarding necessity.

It is therefore difficult to reconcile surveillance for the purposes of detecting loitering with the test of urgent or strict necessity. From initial collection of biometric data to storage to comparisons with databases, interferences with individual's privacy and data protection rights arise at virtually every stage of the process and can be appropriately considered intrusive.

Justifying such intrusions on the basis of petty crime or civil wrongs being a strictly necessary measure would deprive the test of all meaning.

### 1.4.2 EU Law

Article 8(1) of the Charter of Fundamental Rights of the European Union provides that every person has the right to the protection of their personal data. As regards the collection and processing of biometric data, this is regulated by Article 9 GDPR and, in the case of law enforcement authorities, Article 10 of the Data Protection Law Enforcement Directive ('LED').

83 **Ibid.**
84 **BDSG,** s4(1)(3).
85 **BDSG,** s22(1)(1)(a).
86 **BDSG,** s22(1)(1)(b).
87 **BDSG,** s22(1)(1)(c).
88 **BDSG,** s22(1)(1)(d).
89 **BDSG,** s22(1)(2)(a).
90 **BDSG,** s22(1)(2)(b).
91 **BDSG,** s22(1)(2)(c).
92 **s15a(1) PolG NRW;** Art. 33(1) PAG (Bavaria).
93 **BPolG,** s26(1).
94 **BPolG,** ss 21(1), 28.
95 **BVerfG,** Decision of 14 July 1999 - 1 BvR 2226/94, para. 270; BVerfG, Decision of 23 February 2007 - 1 BvR 2368/06, para. 51.
96 **See supra** (n 31).
97 **Deutscher Bundestag,** 2020. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Torsten Herbst, Frank Sitta, Oliver Luksic, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/16870 – Sicherheit in Zügen und an Bahnhöfen avaialble at https://dip21.bundestag.de/dip21/btd/19/174/1917436.pdf, page 6.

Under Article 9 GDPR, the collection and processing of biometric data is lawful only in particular circumstances, namely where the data subject has consented to the collection and processing or such activity is necessary for reasons of substantial public interest.[98]

Where the latter exception is invoked by a data controller, collection and processing must be proportionate to the aim pursued and appropriate measures must be put in place to safeguard the fundamental rights of the data subject.[99]

Under Article 10 LED, biometric data collection and processing is allowed only where 'strictly necessary' for the specific purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties.[100] As the strict necessity test comes from the case law of the CJEU,[101] it must be interpreted in line with principles of EU as opposed to domestic law.[102]

The Article 29 Data Protection Working Party have expressed that 'strict necessity' requires further interpretation, as the case law of the CJEU has not clarified its meaning, and in the meantime have concluded that the term must be understood as 'a call to pay particular attention to the necessity principle'.[103]

Biometric collection can also be done only so long as appropriate safeguards have been put in place to protect the fundamental data rights of data subjects.

The collection and processing must also be authorised by the law of the Member State to protect the vital interests of the data subject. It is worthwhile noting from these requirements that, unlike the GDPR, the LED does not require the consent of the data subject for processing personal data.[104]

Outside the scope of law enforcement, in Michael Schwarz v Stadt Bochum[105] the European Court of Justice confirmed that a data subject's consent is undermined if they do not have a real choice of objecting to the processing of their data.[106]

With this in mind, it is difficult to see what scope for consent there can be regarding biometric mass surveillance by private and state bodies in public or publicly-accessible spaces, such as train stations, which many citizens depend on and have little choice but to use, whether they object to their data being collected or not.

Without adequately sourcing a data subject's informed consent, they may have no idea that their personal data is being collected, which personal data this collection extends to, who is collecting the data, or what purposes the collection is for.

This has subsequent implications for the data subject's Article 1 EUChFR rights and Article 8 ECHR right to respect for private and family life. Legal questions of proportionality have also been raised regarding Cologne's vast networks of biometric cameras.

It is estimated that 200,000 people a day are observed around the cathedral and station, with the recordings retained for 14 days so as to preserve evidence for criminal notifications – however in 2017 only 85 archiving processes were carried out for this purpose.

This would infer that the number of offences captured by the cameras is microscopic in comparison to the number of people whose data is collected and processed (and therefore whose data protection rights are infringed upon) on a daily basis.

Furthermore, the crime figures presented by the police to the Administrative Court indicate that the most highly reported crimes taking place in central Cologne include pickpocketing, robbery, and drug offences.[107]

In assessing the proportionality of these surveillance measures, it must be questioned whether cameras are more appropriate in addressing these crimes than less onerous and less personally invasive traditional methods of policing.

More importantly, it must be questioned whether these offences are significant enough in terms of criminality to justify derogation from general data protections and render biometric data collection 'strictly necessary'.

98 **Regulation (EU) 2016/679 of 27th April 2016** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L 119/1 ("GDPR"), Arts 9(2)(a) and 9(2)(g).

99 **Ibid.**

100 **Directive (EU) 2016/680 of 27th April 2016** on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data [2016] OJ L 119/89 ("LED"), Art 10.

101 **Joined Cases C 293/12 and C 594/12 Digital Rights Ireland Ltd v Minister for Communications,** Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] para 52 et seq.

102 **C-524/06 Huber v Federal Republic of Germany,** [2008] European Court Reports 2008 I-09705, para 52.

103 **European Commission,** Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178, pp 7-8.

104 Ibid.

105 **C-291/12 Schwarz v Stadt Bochum** (CJEU, 2013) 2 C.M.L.R. 5.

106 **Ibid,** para 32.

107 **20 L 2340/19,** supra (n 12) paras 30-38.

### 1.4.3 European Convention on Human Rights

In S and Marper v UK,[108] the European Court of Human Rights ('ECtHR') held that the blanket and indiscriminate processing and retention of biometric data constituted a disproportionate interference with the rights enshrined in Article 8(1) ECHR.[109] The use of such cameras provides prime infrastructure to facilitate the indiscriminate collection of intrusive data. Such cameras therefore raise interferences with data protection and privacy rights at every stage of their use, from collection to processing to retention.

Notwithstanding the limited capacity of the cameras to tackle crime, one must also consider the impact on law-abiding citizens exercising their fundamental rights, such as the right to Freedom of Expression under Article 10 ECHR and the right to Freedom of Assembly and Association under Article 11 ECHR.

As expressed by the German Constitutional Court in the Census[110] judgement of 1983, a person who assumes that participation in a public meeting is officially recorded by state actors may choose to exercise their rights differently than if they were not being recorded, or indeed might not exercise their rights at all, having subsequent implications and significant ongoing impacts not only for the political engagement of the individual, but also for the democratic constituent community as a whole.

### 1.4.4 International Human Rights Law

Germany signed the International Covenant on Civil and Political Rights ('ICCPR') on 9 October 1968 and ratified it on 17 December 1973.[111] Article 17 of the ICCPR provides for the protection of the fundamental universal right to privacy as follows:

**Article 17. (1). No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2). Everyone has the right to the protection of the law against such interference or attacks.**

The UN Special Rapporteur on Privacy, Professor Joe Cannataci, criticised Germany, amongst others, for adopting laws that attempt to appear tougher on security concerns but legitimise 'largely useless, hugely expensive and totally disproportionate measures which are intrusive on so many people's privacy [...].'"[112] He also raised concerns, in respect of multiple nations, regarding the use of immense centralised databases storing biometric data, and highlighted that such data is by definition inseparably linked to the lives of persons affected.[113]

Although the report from Cannataci's country visit to Germany was not submitted in time for consideration by the UN General Assembly, the associated end of mission statement stated that Germany seems to be missing robust oversight bodies which

are sufficiently empowered and resourced to 'knock on the doors' of state authorities, identifying a lacuna in regard to oversight by the competent DPAs.[114]

This is also reflected in our findings, particularly in respect of the duration and limited remedies associated with the Hamburg DPA's handling of Clearview AI.

This gives further weight to proportionality concerns, not only in the scope and intrusiveness of biometric mass surveillance but also in regard to the competence of those entrusted with protecting privacy in Germany.

### 1.4.5 'Biometric-Ready' Cameras

Whilst mass camera surveillance is not new,[115] such systems are increasingly outfitted with hardware and software that allows for live biometric analysis.[116]

Although any imagery, even low-resolution images, can be subject to biometric processing, the deployment of high-tech cameras whose primary function is the collection of biometric data is noteworthy.

Cameras observing public spaces can now not only observe what occurs in a particular place but also identify individuals and access their personal information in real time. Their use can serve to normalise the covert and indiscriminate collection of personal data.

108 **S and Marper v The United Kingdom,** Applications nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008).
109 **Ibid,** para. 125.
110 **BVerfG,** Urteil des Ersten Senats vom 15 Dezember 1983 – 1 BvR 209/83, available at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html
111 **See UN Human Rights Treaty Body Database for Germany.** Available at: https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=66&Lang=EN
112 **UNHRC,** 'Report of the Special Rapporteur on the right to privacy' (6 September 2017) A/HRC/34/60, para 55.
113 **OHCHR,** 'The Right to Privacy in the Digital Age' (3 August 2018) A/HRC/39/29, Available at: https://undocs.org/A/HRC/39/29 para 14.
114 **UNHRC,** Germany: UN expert says "excellent foundations for privacy protection" but gaps remain. (2018) p 2.
115 **Surveillance Studies Network,** 'A Report on the Surveillance Society' (2006) available at https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf
116 **See section** 1.3.1.

#### 1.4.5.1 The right to dignity

The right to dignity underpins all fundamental rights. At the EU level, Article 1 of the European Charter of Fundamental Rights ('EUChFR') identifies the right to dignity as an inalienable right that must be protected.

In Germany, Article 1 of the German Constitution enshrines the right to human dignity and recognises the right to dignity as the basis of human community and the enjoyment of peace and justice.[117]

Article 1 has been read in conjunction with Article 2, the right to free development of personality, to construct the proto-right of respect for human personality (das allgemeine Persönlichkeitsrecht) by Germany's Constitutional Court in the seminal Lebach case.[118]

In analysing the capacity for a surveillance regime to respect the right to dignity, the fundamental question is whether it restricts an individual's ability to lead a dignified life.

It is in the very nature of such biometric-ready cameras that they are to watch over countless people in real time and avoid the awareness or cooperation of the individuals whose biometric data is being processed.

The capacity to have multiple users access streams as well as the capacity for high-resolution image processing means that individuals will have no meaningful sense of how many people are watching them at a given time and at what point they are no longer being observed.

Additionally, the processing carried out by such cameras involves an unascertainable level of scrutiny; technical capacity varies, and therefore it may be unclear to what degree of detail one's behaviour is being processed.

### 1.4.5.2 Structural Discrimination

Algorithms are deployed, often in real time, to identify, monitor, and characterise the behaviour of individuals and crowds in search of behaviour deemed relevant to whoever is observing.

The combination of such algorithms with cameras capable of using them to process biometric data in real time establishes an unprecedented capacity for behaviour analysis. This, however, appears to affect some individuals more than others in that it is deployed more against some individuals as a result of their perceived association with social, economic, or racial groups. With biometric-ready cameras being increasingly relied on to make impactful decisions, their potential to contribute to structural discrimination is a cause for concern.

The innate purpose of such cameras is to assist in the classification of individuals as suspicious or risky. Bias in algorithms, neural networks, and other artificial intelligence (AI) technologies is intrinsically linked to their training and input-data.

There is often an assumption that computer-generated assessments and predictions are accurate and trustworthy, but algorithmic bias is a widely recognised phenomenon.[119] Most AI systems have been found to have a higher rate of false positive matches for minority ethnic faces.[120]

AI that attempts to identify emotional states off of facial data, which has already been considered unworkable,[121] also have been identified to have racially biased influences.[122] This has more broadly been considered to contribute to structural discrimination and over-policing.[123]

However, even if algorithmic bias were addressed beyond fault, concerns regarding structural discrimination would not be alleviated due to the discriminatory ways in which these technologies are frequently deployed.

Both on part of public authorities and private actors, it has been argued that there is an innate presumption that all individuals being observed carry the potential to be wrongdoers of some kind, creating an "ethos of suspicion".[124]

This may contribute to a socio-political landscape where those with state authority or capital have the power to observe, those that don't have no choice but to be observed.

This goes to the "untouchable core" that is the right to dignity, which is the essence of the right to privacy and freedoms of expression and assembly.[125]

### 1.4.5.3 Proportionality

The intrusive scope of camera capabilities, paired with their broader social impacts, weigh into concerns of proportionality raised by individual citizens and civil society. The UN High commissioner for Human Rights reported in 2018:

**"The creation of mass databases of biometric data raises significant human rights concerns. Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data."[126]**

With the purpose of their installation being based on broadly drafted legislative grounds, the biometric video surveillance regimes being increasingly rolled out across Germany evade the need to demonstrate a specific purpose of their installation at the particular places in which they are established.

In general terms, there seems to be an institutional assumption that the use of biometric-ready cameras, with limited oversight or public awareness of the balancing of relevant factors, is justified on the broad assumption, which has been challenged by this research, that more surveillance equals less crime.

However, even if it did, the concerns regarding fundamental rights and the right to dignity that underpins them, as outlined above, would apply regardless of any link to efficacy.

---

117 **Basic Law for the Federal Republic of Germany** (Grundgesetz), Art 1(2).

118 **BVerfG,** Urteil des Ersten Senats vom 5. Juni 1973 – 1 BvR 536/72, para 10 et seq.

119 **Hao, K.,** 'This is how AI bias really happens — and why it's so hard to fix' (MIT Technology Review, 2019). Available at: https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix

120 **Hao K,** 'A US Government Study Confirms Most Face Recognition Systems Are Racist' (MIT Technology Review, 2019) https://www.technologyreview.com/2019/12/20/79/ai-face-recognition-racist-us-government-nist-study

121 **Korte A,** 'Facial-Recognition Technology Cannot Read Emotions, Scientists Say' (American Association for the Advancement of Science, 2020) https://www.aaas.org/news/facial-recognition-technology-cannot-read-emotions-scientists-say

122 **Rhue, Lauren,** Racial Influence on Automated Perceptions of Emotions (November 9, 2018). Available at SSRN: https://ssrn.com/abstract=3281765 or http://dx.doi.org/10.2139/ssrn.3281765

123 **European Union Agency for Fundamental Rights,** 'Facial recognition technology: fundamental rights considerations in the context of law enforcement" (2019) available at https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

124 **Minaj, J., & Bonnici, J..** Unwitting subjects of surveillance and the presumption of innocence. (2014) Computer Security and Law Review, 30(4), p. 421; Duff, A. Who must presume whom to be innocent of what? (2013) Netherlands Journal of Legal Philosophy, 42(3).

125 **Thielbörger, P.,** The "Essence" of International Human Rights, (2019) Germany Law Journal, 20, 924-939, p 938.

126 **The right to privacy in the digital age,** supra (n 112).

# 2. FINGERPRINTS ON PERSONAL IDENTITY CARDS

**On November 5, 2020, the Bundestag (German federal parliament) decided that fingerprints are mandatory in German identity cards ('ID'). From August 2, 2021, everyone will be required to have the prints of their two index fingers saved on the chips of the cards when applying for an ID.**[127]

Local authorities have also been setting up automated systems of issuing IDs, in order to minimise face-to-face contact during the pandemic, which require fingerprint verification.[128] FOI requests to obtain more information about this process were firstly rejected for "security reasons"[129] but a different request to the same authority was approved and documents were issued.[130]

The authorities claim that the fingerprint data is stored safely and locally, but, security concerns aside, this was noted as an instance of inconsistency and a lack of forthcomingness on the part of public authorities.

The German civil society organisation Digitalcourage launched a campaign, 'Perso ohne Finger' ('ID without finger'), against the implementation of this requirement, listing concerns about the ethos of suspicion this promulgates, along with concerns about access and long-term impacts on democratic values.[131]

127 **Ebelt F,** 'Union Und SPD Haben Fingerabdruck-Pflicht Beschlossen' (Digitalcourage, 2020) https://digitalcourage.de/blog/2020/fingerabdruck-pflicht%20beschlossen-persoohnefinger

128 **Das Ausweisterminal / Kern** – Your technology partner (SmartTerminals) available at https://www.smart-terminal24.com/de/systeme-software/systeme/ausweisterminal.html

129 **Stadt Langenhagen,** 'Anfrage #205071: Einwilligungserklrung Abholstation und Datenschutzinformation' (14 December 2020) available at: https://fragdenstaat.de/anfrage/abholautomat-fur-ausweise

130 **Stadt Ludwigsburg,** 'Anfrage #205072: Abholautomat für Ausweise' (5 December 2020) available at: https://fragdenstaat.de/anfrage/abholautomat-fur-ausweise-1

131 **'Perso Ohne Finger'** (Digitalcourage 2020) available at: https://aktion.digitalcourage.de/perso-ohne-finger

# 2. 1 Analysis

Fingerprints in ID cards are by no measure a new phenomenon. This policy is part of Germany's attempted implementation of recent EU Regulations.[132] However, the impacts of the announced requirements raise further issues under European law and policy when analysed in context.

### 2.1.1 Human rights concerns

Fingerprints render individuals traceable for life. Measures which individuals may take to remain anonymous, for example, in order to anonymise their attendance at a protest, do not protect against fingerprint identification.

An increased reliance on biometrics for identity verification poses unique risks. Identity theft based on biometrics is extremely difficult to remedy and has serious implications on an individual's rights.[133]

The right to privacy is broad and applies not only to the contents of communications but also to personal development and our ability to communicate parts of ourselves to the outside world.[134]

Even the analysis and aggregation of metadata, such as data relating to where and when an ID card was scanned, can give an insight into an individual's behaviour, social relationships, and private preferences that can be even more intrusive than monitored communications.[135]

It therefore stands that an increase in reliance on fingerprint identification restricts the ability of individuals to exercise anonymity in public should they wish to do so.

Consequently, the retention of fingerprint data by the State also has follow-on effects on rights including but not limited to the following:

1. The universally recognised right to privacy;[136]
2. The European-wide recognised right to protection of personal data;[137]
3. The universally recognised right to freedom of expression;[138]
4. The universally recognised right to freedom of thought, conscience, and religion;[139]
5. The universally recognised right to freedom of peaceful assembly;[140]
6. The universally recognised right to freedom of association;[141]
7. The universally recognised right to take part in public affairs; and[142]
8. The universally recognised right to freedom of movement,[143] *inter alia.*

### 2.1.2 Consent

With German passports already requiring biometric data through fingerprints,[144] all forms of state ID mandate the collection of biometric data, as drivers' licences are not legally accepted forms of ID.[145] German citizens will have no constructive choice but to register their fingerprints, as government ID cards are mandatory.[146]

In Michael Schwarz v Stadt Bochum, the CJEU held that citizens could not be deemed to have consented to the collection of biometric data where such processing is the only way of accessing a service, such as travel.[147]

The CJEU did, however, consider the requirement for fingerprints in the Schwarz case legitimate in spite of the lack of consent.
This reflects the qualified nature of the rights under the EUChFR and how they must be assessed in light of their function in society.[148]

However, the Schwarz decision can be distinguished on the basis that government ID cards apply beyond the scope of international travel and affect every German citizen.

It remains the case that the capacity to object against biometric IDs has been erased by this policy. Questions will therefore undoubtedly be raised as to how this can be balanced in light of the alleged societal functions of mandatory biometric IDs.

### 2.1.3 Access Extension

Concerns also exist in respect of the circumstances in which access to this data can be extended. For example, as of 2017, German police are permitted to automatically access biometric data from passports and government ID cards.[149] However, the risk extends beyond police access.

The regulation requires[150] global interoperability in respect to machine readability as required by the International Civil Aviation Organization.[151]

---

132 **Regulation (EU) 2019/1157** of the European Parliament and of the Council of 20 June 2019.
133 **The right to privacy in the digital age,** supra (n 112), rec 14.
134 **Pretty v UK (2002)** 35 EHRR 1, para 61.
135 **The Right to Privacy in the Digital Age** supra (n 112), para 7.
136 **ICCPR Art. 17,** UDHR Art. 12, ECHR Art. 8, EUChFR Art 7.
137 EUChFR Art. 8.
138 **ICCPR Art. 19,** UDHR Art. 19, ECHR Art. 10, EUChFR Art. 11.
139 **ICCPR Art. 18,** UDHR Art. 18, ECHR Art. 9, EUChFR Art. 10.
140 **ICCPR Art. 21,** UDHR Art. 20, ECHR Art. 11, EUChFR Art. 12.
141 **ICCPR Art. 22,** UDHR Art. 20, ECHR Art. 11, EUChFR Art. 12
142 **ICCPR Art. 25,** UDHR Art. 21, ECHR Art. 9, EUChFR Art. 39 and 40.
143 **ICCPR Art. 12,** UDHR Art. 13, ECHR Art. 2, EUChFR Art. 45.

As such, the biometric data on German government ID cards could in theory be accessed by actors in countries where data and civil rights protections are not enforced. Moreover, the regulations advise "caution" in regard to collaborations with external service providers.[152] This means that private companies may have access to such biometric data, notwithstanding the specifics of such collaborations remain unclear.

The legal, political, social, and ethical implications of a mandatory biometric state ID requirement are extensive and not yet fully known. Due to the compulsory nature of government ID cards, the required inclusion of fingerprint data relies on the mass collection, processing, and storage of biometric data and thereby circumvents the requirement of consent.

The implications of permanence and access extension equally raise questions of transparency and informational autonomy squarely invoking numerous authoritative binding international and regional human rights instruments as detailed above.

Both European and domestic law generally assume that requiring the collection and processing of biometric fingerprint data pursues legitimate interests, whereas data protection concerns, and other fundamental rights implications, appear to receive less focus.

144 **Bundesdruckerei,** ePASS Fibel (2007) available at https://web.archive.org/web/20101031204925/http://bundesdruckerei.de/de/produkte/produkte_dokument/dok_persausw/download/produkte_sicherheit.pdf

145 **'Namensänderung' (Nuernberg.de)** https://www.nuernberg.de/internet/ordnungsamt/namensaenderung.html

146 **Gesetz über Personalausweise und den elektronischen Identitätsnachweis** (Personalausweisgesetz - PAuswG) 2009, s1.

147 **See supra n 104,** para 32.

148 **Case C 543/09 Deutsche Telekom** [2011] ECR I 3441, para 51.

149 **Gesetz zur Förderung des elektronischen Identitätsnachweises,** G 5702, 14 July 2017.

150 **Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement,** OJ L 188, 12.7.2019, rec 23.

151 **Machine Readable Travel Documents,** Doc 9303 (International Civil Aviation Organisation, 2015).

152 **See supra (n 146)** rec 42.

# 3. ONLINE AGE AND IDENTITY 'VERIFICATION'

**HooYu Identify is a UK-based customer onboarding and identity verification platform which verifies identities through a combination of digital footprints, metadata, ID documents, and biometrics.**[153]

**Its use in Germany was approved by the German Commission for the Protection of Young People in the Media (Kommission für Jugendmedienschutz) in January 2021 as a suitable age verification system.**[154]

Such a system would require those wishing to access adult sites, such as gambling operators and other adult entertainment websites, to verify their identities via biometric 'liveness' detection, which involves taking pictures of themselves and an ID document. It therefore stands that HooYu would be identifying individuals through biometric analyses and tying them to particular online activities.

Thousands if not millions of adults would therefore be required to submit to biometric processing on a massive scale in order to access certain online activities, the demand for which will likely increase significantly in light of the COVID-19 pandemic as various services and activities move to being entirely online during this period at the minimum.

Whilst the system is designed to identify adults, the very nature of the process would mean that the data of children and young people would also be processed by HooYu.

153 **See** https://www.hooyu.com/h

154 **'HooYu Biometrics approved in Germany' (Biometric Update, 2021)** https://www.biometricupdate.com/202101/hooyu-biometrics-approved-in-germany-new-ui-tools-launched

## 3.1 Analysis

Article 6(1)(a) GDPR provides that the processing of personal data is lawful only if the data subject has given their consent to such processing. Whilst adults wanting to access restricted websites *prima facie* will have a choice over whether they submit their biometric data or not in exchange for admittance, applying *Schwarz* reveals that there is only an illusory choice, as the only alternative for those unwilling to submit their biometric data is to not use the online service at all.

This predicament is particularly apparent in light of the COVID-19 pandemic and the concomitant closure of physical high street premises, such as those offering gambling/banking services, which has limited adults to online access only. Matters of consent aside, there is also the possibility that, in seeking to improve the protection of young people online, the data of adults is put at greater risk, and the data of young people trying to access such services may also be put at risk.

Events of recent years, from the unauthorised harvesting and use of people's online personal data to influence national elections – as was seen in the case of Cambridge Analytica[155] – to the leaking of millions of user details from dating websites such as Adult Friend Finder,[156] have shown the susceptibility of personal information on the internet to interception and misuse.

A reported data breach in 2019 of 28 million records of fingerprint and facial recognition data at biometrics company Suprema, used by London's Metropolitan Police, defence contractors, and banks, has shown that biometric data is not immune to these risks.[157]

Although the precise scope of how this stolen data might be used is not yet fully understood, what is appreciable is that once biometric data is compromised, it cannot be changed in the same way as passwords or credit card details.

With this vulnerability in mind, one can imagine the possible dangers of uploading national identification documents to the internet, the most evident risks being counterfeiting and identity fraud. While biometric data sharing does not automatically entail biometric surveillance, there is always the danger that widespread biometric data traffic will fall prey to cybersecurity breaches that enable data to be intercepted by third parties and used for surveillance purposes.

These hazards may be compounded when such documents are paired with social media data that can give an insight into an individual's personality, psychology, and language patterns. With users potentially numbering in the millions, age verification companies are likely to be prime targets.

There may also be additional temptations where, rather than losing valuable data to criminal enterprise, it is actively sold to third parties for profit. As discussed above, a further danger is that the use of age verification technology for services such as online banking will render biometric data collection commonplace, desensitizing people to the long-term risks.

155 **Carole Cadwalladr & Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' (The Guardian, 17 March 2017)** www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

156 **Zack Whittaker, 'AdultFriendFinder Network Hack Exposes 412 Million Accounts' (ZDNet, 13 November 2016)** www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users

157 **Zak Doffman, 'New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report' (Forbes, 14 April 2019)** www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report

# 4. COVID-19 RESPONSES

**The emergence and outbreak of the global COVID-19 pandemic has also created a perfect storm for pushing forth more surveillance and biometric data collection in the name of public health. As always, questions of proportionality and legitimate interest arise.**

However, concerns about dealing with the pandemic have created conditions where deployments of biometric mass surveillance are being used beyond their purported remit and to a much more invasive extent without adequate oversight and safeguards.

The biometrics industry has seen a surge in demand following the COVID-19 outbreak, with biometric facial recognition being promoted as an alternative to fingerprint scanners for workplaces now that it is adapted to work with masks.[158]

Germany's Scandinavian Park mall has chosen contactless fever screening technology from Dermalog, another biometrics firm, to improve health protection measures and "ensure a seamless customer experience", the company announced.[159] By detecting body temperature from a distance, Dermalog's fever detection camera can significantly reduce infection risk, the company says.

Additionally, Cognitec has been piloting facial recognition technology which applies matching algorithms to masks which it claims have a detection rate "five times higher" than similar software for faces covered by masks.[160]

The new developments on mask-tolerant matching algorithms are to be integrated into Cognitec's existing software which allows for images to be compared to larger databases and are advertised to generate real-time alerts.[161]

## 4.1 Analysis

As outlined above, Article 9(1) GDPR prohibits biometric data collection unless an exception at Article 9(2) applies. One such exception provides that collection is lawful where it is necessary for reasons of public interest in the area of public health, such as protecting against cross-border threats.

Ascertaining whether the Scandanavian Park mall deployment is necessary and therefore lawful is challenging. As the Council of Europe expressed in a recent Joint Statement,[162] there is currently an absence of evidence of the efficacy of the technological tools being used to combat COVID-19 and whether the benefits are worth the societal and legal risks.

As outlined in the same Joint Statement: "large scale personal data processing can only be performed when, on the basis of scientific evidence, the potential public health benefits of such digital epidemic surveillance, including their accuracy, override the benefits of other alternative solutions which would be less intrusive."[163]

It follows from this that, without sufficient scientific evidence, large scale data processing cannot be conducted at all.

With vaccination programmes gathering pace around the world, a question remains over how long the pandemic will remain a cross-border threat to public health and therefore a lawful basis for the use of biometric technologies under Article 9(2).

A risk this poses is that, so long as the COVID-19 pandemic continues to threaten (or be said to threaten) the public, it can be used as a rhetorical carte blanche, evading established domestic and European legal principles.

A key component of this risk appears to be a lack of robust enforcement of data protection laws in the COVID-19 context.

Where this is allowed to continue without proper respect for the necessary safeguards and controls, a further danger is that biometric deployments become normalised during the pandemic period, eroding public awareness of consent and proportionality requirements by force of habit.

Whilst the challenges posed by the pandemic are difficult and unprecedented, measures put in place must not put rights at greater risk in the long term.[164]

## 4.2 The Convenience of Control

It is worth noting the implications of a purportedly "seamless" experience in regard to biometrics, which is the offer often put forward by the companies selling the systems. If the seams in question are checks or instances in which customers have to consciously decide whether to submit to the processing of their personal data, such an approach may raise concerns in respect of consent. Business models mitigating individual input with respect to authentication are a growing phenomenon.[165]

More generally, market research into biometrics has focused on the lack of "hassle" that the use of biometrics provide, such as by not having to remember a passcode or PIN, and eliminating the need to remember ID numbers, passwords, or other authentication methods.[166]

This raises questions as to what the costs of less hassle are, with the risks of removing customers' consent and awareness being at the forefront.

158 **Burt C, 'Biometrics Industry Seeing Higher Demand And Adapting Technology To Help Outbreak Mitigation (Biometric Update, 2020)** https://www.biometricupdate.com/202003/biometrics-industry-seeing-higher-demand-and-adapting-technology-to-help-outbreak-mitigation

159 **'Retailers Rely On DERMALOG's Temperature Screening' (Dermalog, 2020)** https://www.dermalog.com/news/article/retailers-rely-on-dermalogs-fever-screening

160 **'Facing the mask challenge' (Cognitec)** https://www.cognitec.com/files/tao/downloads/Cognitec-Facing-the-Mask-Challenge.pdf

161 **'New Mask-Tolerant Matching Algorithm And Age Estimator' (Cognitec, 2021)** https://www.cognitec.com/news-reader/cognitec-product-releases-2021.html

162 **Alessandra Pierucci & Jean-Philippe Walter, 'Joint Statement on Digital Contact Tracing'** (Council of Europe Committee of Convention 108, 28 April 2020) p 2.

163 **Ibid** p 3.

164 **Council of Europe, 'Joint Statement on the right to data protection in the context of the COVID-19 pandemic** (30 March 2020) https://rm.coe.int/covid19-joint-statement/16809e09f4

165 **See e.g 'Biometric Technology Enabling Seamless Airport Vision' (Future Travel Experience, 2015)** https://www.futuretravelexperience.com/2015/07/biometric-technology-driving-seamless-airport-vision

166 **VISA, 'Goodbye, Passwords. Hello, Biometrics' (2017)** https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-biometrics-payments-study.pdf

167 **The right to privacy in the digital age,** supra (n 112).

As mentioned above, increased reliance on biometric verification can create a robust and extremely difficult to remedy infrastructure for identity theft.[167]

Moreover, as the 'seamlessness' of biometrics innately requires less stages in a service where active input or consent is required, organisations using biometrics can unilaterally create means by which biometric data is covertly collected and processed. Its use may normalise apathy vis-à-vis biometric processing as well as dilute the need to justify intrusions on the basis of demonstrable necessity.

The established legal principles in relation to biometric data processing, particularly where consent is not obtained, emphasise strict necessity and proportionality, not of reasonableness or convenience.

It comes down to the convenience that such control provides, characterised by externalised state or private access to our personal biometric data – the question is whether that convenience is really worth the unprecedented and often as yet unrealised risks.

# 5. CONCLUSION

**This section has identified four examples of how biometric mass surveillance operates in Germany. The use of facial recognition in public spaces has not become a prevalent phenomenon overnight. Rather, the current facial recognition surveillance regime is the product of years of infrastructure development, political tides, and engagement from the private sector.**

Given the open ties between private actors and public bodies, facial recognition has gradually evolved beyond a tool for addressing purportedly urgent issues of public interest to a broad market which is extending into the surveillance of petty crimes and non-criminal acts.

This was the result of developments both in practice and in law. Moreover, the interplay between state bodies, private actors, and supervisory authorities appears to have developed so that the burden often lies on individual citizens and civil society to actively pursue the protection of the fundamental democratic rights and values that such surveillance regimes engage.

Biometrics in German identity cards, by virtue of their compulsory nature, necessitate the indiscriminate collection of biometric data en masse. These are not without their risks, given that fundamental rights are innately engaged and access extension remains a concern largely unaddressed at the time of writing.

Another issue is also that this increased reliance on biometric data for identity verification is a double-edged sword. Its purported security benefits, once breached, can severely harm data subjects, given the ever-present risks of data security and identity theft.

The analysed measures seeking to protect young people online pursue a legitimate aim, but little focus has been found regarding the risks which the reliance on such measures pose for the biometric data of adults (and potentially young people who may attempt to use the system).

We have identified a shift in reliance on biometrics for verification that, with no viable alternative, removes constructive consent vis-á-vis biometric processing.

Although our analysis points towards certain risks, such as hacking and the commercialisation of biometric data, this remains an area in which further risks and harms may be discovered later down the line.

Finally, in light of the COVID-19 pandemic, we have seen states across Europe using the mass collection of biometric data in pursuance of public health goals.

In Germany, this has taken various forms including facial recognition technology aimed at identifying mask-wearers as well as use of various biometric processing tools by private actors in purported pursuit of 'seamless' experiences in publicly accessible spaces.

Although novel and innovative from a technical standpoint, this does not negate the intrusive and far-reaching impacts on fundamental human rights.

This applies not only as a concern now, but even more so in future. The big question on this point is to what extent these measures, and the culture of reliance on biometric mass surveillance that comes with them, will be in place after the pandemic no longer poses the threat it poses in 2021.

# INTRODUCTION TO THE NETHERLANDS COUNTRY STUDY FROM EDRI:

**This research into biometric mass surveillance in the Netherlands reveals that, despite widespread views of the Netherlands being a welcoming and tolerant country, these adjectives do not apply to the vast range of unlawful and rights-violating biometric practices by police, municipalities, and private actors.**

The deployments investigated in this research are riddled with problems of a lack of transparency, lack of oversight, meaningless checks and balances, and a failure to perform adequate (if any) data protection assessments.

Worse still, in the majority of use cases identified, their use is inherently disproportionate – i.e. most of the examples analysed violate the fundamental rights of a large number of people for seriously unreasonable purposes, such as convenience (ordering fast food, reducing queues) or monitoring petty crimes (shoplifting in supermarkets, transport violations, or detecting people that are trying to avoid a carnival ban).

Even where use cases are pursuing a legitimate aim, the research has revealed that, under law, authorities should have used a less invasive available alternative – and, in most cases, the uses were also not actually effective for the aim sought.

One particularly chilling set of examples is the rise of so-called 'Living Labs' in several Dutch cities. These collaborations between police, municipalities, and private entities – often giving huge amounts of data to private companies – place whole cities under the status of experimental test subjects.

They use various forms of data – for example, combining biometric data with social media data – for purposes such as inferring if young people are hanging out on a street and predicting their future life outcomes on this basis. As well as the blatant intrusion into people's lives and dignity, these labs are usually happening without the knowledge or consent of the individuals or communities being surveilled.

Another shocking example reveals the police using financial incentives and dark patterns to nudge companies and citizens into sharing private surveillance and "smart" doorbell camera footage with police for facial recognition analysis.

Not only does this raise serious ethical concerns, it is also a brazen attempt to circumvent the rules governing the police's ability to collect such data, making citizens complicit in the unlawful biometric mass surveillance of their communities.

Underpinning these biometric mass surveillance practices by police forces in the Netherlands, such as through the use of the notorious CATCH facial recognition software, is the systematic violation of people's data and privacy through biometric mass surveillance databases.

For example, police have been found to hold on to the biometric data of not just criminal convicts, but also suspects for between twenty and eighty years – and fail to remove this data even when someone is found not guilty or when investigations have revealed that the police have no legal basis for holding this data! Such practices are even more concerning where they have been deployed against foreign nationals, who are included in biometric databases solely for the reason of being an "alien".

They are thus treated as inherently suspicious because of their nationality, against a wider backdrop of substantiated racial and ethnic profiling by Dutch police forces, showing the huge potential for discriminatory use of biometric mass surveillance practices and infrastructures.

Furthermore, the inherent limitations of biometric mass surveillance technologies have been revealed in this case study on the Netherlands, with the Zeeland-West-Brabant Court acquitting a suspect against whom the only evidence was a purported facial recognition match. No improvements in the accuracy of the technology will be able to overcome the fact that biometric technologies are unable to conclusively provide a match.

Across the use cases highlighted in the Netherlands, this research also reveals the systematic misuse of exceptions in existing national and European law, the pretence of a 'trial' or 'experiment' as a pretext for violating people's rights, and the persistent collection and storage of people's biometric data without a legal basis.

These many reasons are central to EDRi's call for why the EU so urgently needs to fully and tangibly ban biometric mass surveillance practices.

# THE NETHERLANDS

**This country-specific section provides an overview of the various deployments of biometric data surveillance technologies in the Netherlands.**

Whilst biometric surveillance includes an array of data gathering and harvesting techniques, such as DNA or fingerprints collection, facial geometry recognition, and voice, retina, or iris analysis, this section mainly focuses on facial recognition technology, which is used most frequently.

The deployments are divided into three categories, as follows: **(1)** deployments by public state entities, **(2)** deployments by private corporate entities, and **(3)** so-called 'Living Labs' which tend to involve both public state and private corporate entities.

Some sections are divided further based on the specific examples of the technology being used and its purpose. Following a general factual overview of the three forms of deployments, the report proceeds to analyse the legality of each type of deployment under domestic and international law.

The use of biometric surveillance and wider concerns about the relationship between technology, governance, and human rights are part of an ongoing wider public debate within the Netherlands.

For instance, during the election campaign for the Dutch general election in March 2021, the manifestos of all parties talked about issues relating to privacy and data protection to some extent, while specific reference was made to biometrics in the manifestos of six prominent parties running in the election.[168]

Furthermore, in February 2021, the Dutch government collapsed following the controversy surrounding the so-called 'Toeslagenaffaire', in which over 20,000 families were falsely accused of fraud by the tax authority and forced to repay child benefits based on a discriminatory algorithm.[169]

Biometrics and facial recognition technology in the Netherlands are strikingly widespread, used by both public and private actors, for a wide range of purposes. One thing that particularly stands out is the ambiguous and muddy legal waters of almost every deployment: in most cases, deployments are extralegal or contested by civil society, because actors misuse exceptions in the law and oversight bodies are not given sufficient means to do their jobs properly.

Thus, it can be seen that the use of biometric data surveillance by law enforcement agencies is often ahead of the law so there are few codified rules or precedents dealing directly with it. However, the principle behind the illegality of other surveillance technologies, specifically the universal rights to privacy and dignity, render new technologies unlawful on the same basis.

---

168 **Based on a personal analysis of every manifesto. Analyzed the manifestos of 50PLUS, DENK, Partij voor de Vrijheid, Staatkundig Gereformeerde Partij, Socialistische Partij, Volkspartij voor Vrijheid en Democratie, Christen-Democratisch Appèl, ChristenUnie, Forum voor Democratie, GroenLinks, Partij van de Arbeid, Partij voor de Dieren,** D66.

169 **Gabriel Geiger, 'How a Discriminatory Algorithm Wrongly Accused Thousands of Families of Fraud' Vice (2021) available at:** https://www.vice.com/en/article/jgq35d/how-a-discriminatory-algorithm-wrongly-accused-thousands-of-families-of-fraud

In terms of the applicable legal framework, Dutch regulations concerning data protection are largely derived from the European Union's General Data Protection Regulation (GDPR), applicable from May 2018 and implemented in the Netherlands on the same date.[170]

The GDPR replaced most of the Data Protection Act 2001, a Dutch law which previously provided the main framework for general data protection in the Netherlands. These two pieces of legislation do not deviate from each other in any significant way, so there appears to be continuity in Dutch national laws concerning data protection. Notably, the GDPR does not apply to police activities.[171] These are instead regulated by the LED and the Police Data Act 2007 in the Netherlands.

The national authority tasked with supervisory jurisdiction over matters of personal data is the Dutch Data Protection Authority ('DPA/AP'), which also represents the Netherlands on the European Data Protection Board.

The European Data Protection Board is an independent European Union body which aims to ensure the application of data protection laws throughout the European Union and promotes cooperation between European data protection authorities.[172]

[170] **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); implemented by Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) available at:** https://wetten.overheid.nl/BWBR0040940/2018-05-25

[171] **Ministerie van Justitie en Veiligheid, Handleiding Algemene Verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming (2018), available at:** https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf, p. 29.

[172] **European Union Data Protection Board, 'About EDPB' edpb (2021) available at:** https://edpb.europa.eu/about-edpb/about-edpb_en

# 1. DEPLOYMENTS BY PUBLIC ENTITIES

**Our research has revealed that local authorities in municipalities and police forces in the Netherlands use facial recognition technology and other forms of biometric surveillance in a multitude of ways. The police use several facial recognition databases, generally to identify suspects of crimes.**

Particularly concerning in this instance is that Dutch police forces can obtain access to footage from individuals' and business' security cameras and smart doorbells, some of which film public space.[173]

There are also reports that police are trialing the use of real-time facial recognition technology through smartphone pictures, body cams, and the cloud.[174] Municipalities, on the other hand, only tend to use facial recognition technology in certain instances, for example during carnivals and other large events.[175] A certain number of municipalities also engage in surveillance through so-called 'Living Labs', which are covered in section 3 below.

The use of biometric surveillance by public authorities like the police and municipalities raises particular concerns of data protection, proportionality, transparency, and the protection of fundamental, universally recognised human rights.

**173 Politie Nederland, 'Camera in Beeld' (Thema's, 2020) available at:** https://www.politie.nl/themas/camera-in-beeld.html?sid=07c1d5df-60bf-470a-993f-f9f212c9dd00

**174 For instance, see Elsbeth Stoker, 'CSI in de polder: politie zoekt verdachten met gezichsherkenning' (de Volkskrant 2016) available at:** https://www.volkskrant.nl/nieuws-achtergrond/csi-in-de-polder-politie-zoekt-verdachten-met-gezichtsherkenning~bde94cf6 Wester van Gaal, 'Gezichtsherkenning op de Nederlandse straten: moeten we dat willen?' VICE (2019) available at: https://www.vice.com/nl/article/8xzydz/gezichtsherkenning-op-de-nederlandse-straten-moeten-we-dat-willen

**175 For instance, see Bart Gotink, 'Slimme camera's herkennen elke carnavalsvierder in Korte Putstraat: 'Wie er niet in mag, hebben we er zo uitgepikt' BD (2019)** https://www.bd.nl/den-bosch-vught/slimme-camera-s-herkennen-elke-carnavalsvierder-in-korte-putstraat-wie-er-niet-in-mag-hebben-we-er-zo-uitgepikt~a55f6fdd/?referrer=https%3A%2F%2Fwww.google.com%2F

# 1.1 Dutch police and law enforcement authorities

### 1.1.1 CATCH Facial Recognition Surveillance Technology

Since 2016, the Dutch police use a system of facial recognition technology called CATCH, aimed at identifying suspects or convicts of crimes through a criminal justice database.[176] The database holds the pictures and fingerprints of all suspects and convicts of serious crimes recorded since 2010, as well as people who refused to identify themselves when arrested.[177]

'Serious crimes' are defined as crimes which carry a maximum sentence of four years or more.[178] The database is vast, containing the information of 1.4 million people and containing 2.3 million pictures, all taken in Dutch police stations.[179]

Crucially, this biometric data can be retained for twenty to eighty years, and while the data should be removed if a person is later found to be innocent, in practice, it is unclear if this actually happens.[180]

Indeed, a recent investigation by Dutch online newspaper Nu.nl in March 2021 found that the Dutch police are failing to remove the data of those who are in the CATCH database without a legitimate reason, uncovering that almost 180,000 people might be eligible for removal, but only 14,914 (0.83%) removal requests have been actioned so far.[181]

Remarkably, Dutch police, as well as the Minister for Justice and Security, even recognise that it is likely that tens of thousands of people are in the database without justification.[182] Furthermore, the Nu.nl investigation found that the police failed to carry out a formal assessment of the privacy risks posed by CATCH before its introduction.[183]

Dutch police are also authorised to use the images in the CATCH database for various reasons. In particular, if the police wish to identify someone in camera footage (whether from security cameras, bodycams, or videos sent to them by the public), they can request that facial recognition technology be applied using the CATCH database to generate a potential list of matches. [184]

This can be done without any independent check by a third party on the grounds for the use of the database and facial recognition technology.[185]

The Dutch police claim that this is remedied through the use of two undisclosed "human experts", who are independent from one another and who are said to follow an extensive checklist before concluding that there is a match.[186]

However, there is no evidence provided of their alleged expertise nor any set standard of what experience is required to constitute the requisite standard. The most conservative conclusion found by either of the undisclosed "experts" is given as the final determination and the most far-reaching conclusion possible is that there are 'a lot of similarities'.[187]

This means that the final conclusion can never be that the person the police are trying to identify is in fact the same as the person recorded in the database, only that there are similarities, although in practice whether this means anything depends on what is subsequently done with this private biometric information. This raises more significant questions about the reliability of the technology in informing the ability of police to prosecute crimes to the requisite standard of legal proof.

In 2017, the CATCH system was used 977 times, resulting in 93 matches.[188] In 2018, 82 matches were found out of 961 pictures. Out of 1,027 pictures used in 2019, 8% led to a match.[190]

176 **Paula Hooyman, 'Het ware gezicht van gezichtsherkenningstechnologie' Bits of Freedom (Amsterdam 2019).** https://www.bitsoffreedom.nl/wp-content/uploads/2019/11/het-ware-gezicht-van-gezichtsherkenningstechnologie.pdf

177 **Ibid.**

178 **Ibid.**

179 **Ibid.**

180 **RTL Nieuws, 'Gezichtsherkenning in de openbare ruimte: moeten we daar blij mee zijn?' RTL (2020) available at:** https://www.rtlnieuws.nl/nieuws/nederland/artikel/4997021/gezichtsherkenning-openbare-ruimte-bits-freedom-digitaal-online

181 **Redactie, 'Mogelijk tienduizenden Nederlanders onterecht in database voor gezichtsherkenning' de Volkskrant (2021) available at:** https://www.volkskrant.nl/nieuws-achtergrond/mogelijk-tienduizenden-nederlanders-onterecht-in-database-voor-gezichtsherkenning~b72d2971

182 **Stan Hulsen, 'Tienduizenden mensen mogelijk onterecht in gezichtendatabase van de politie' Nu.nl (2021) available at:** https://www.nu.nl/tech/6121460/tienduizenden-mensen-mogelijk-onterecht-in-gezichtendatabase-van-de-politie.html **Ministerie van Justitie en Veiligheid, Antwoorden Kamervragen over het bericht 'Gezichtendatabase van politie bevat foto's van 1,3 miljoen mensen' (30th of October 2019) available at:** https://www.rijksoverheid.nl/documenten/kamerstukken/2019/10/30/antwoorden-kamervragen-over-het-bericht-gezichtendatabase-van-politie-bevat-foto-s-van-1-3-miljoen-mensen

183 **Stan Hulsen,** Nu.nl (2021).

184 **Julian Huijbregts, 'Nederlandse politie begint met gezichtsherkenning bij opsporing' Tweakers (2016) available at:** https://tweakers.net/nieuws/119105/nederlandse-politie-begint-met-gezichtsherkenning-bij-opsporing.html

185 **RTL Nieuws, 'Gezichtsherkenning in de openbare ruimte: moeten we daar blij mee zijn?' RTL (2020) available at:** https://www.rtlnieuws.nl/nieuws/nederland/artikel/4997021/gezichtsherkenning-openbare-ruimte-bits-freedom-digitaal-online

These are relatively small numbers, especially considering the size of the database and the absolute number of crimes committed in the Netherlands each year, which is around 800,000.[191]

Furthermore, even in the case of a match, there is little guarantee that the match actually concerns the person identified, or that the identity of the person was useful to the police investigation, or that the person was actually guilty of a crime.

Thus, a significant question mark hangs over the practical utility of this technology for crime control, especially in the context of the significant expenditure by the Government of taxpayers' money into this system.

The Dutch police claim that these images are not being used in real time or without good reason,[192] but there have been reports hinting to the contrary. For instance, a few years ago, reports pointed to a new smartphone app being trialled through which officers could directly send pictures to CATCH.[193]

A University of Twente professor has also stated that there are currently trials being conducted using bodycams with real-time facial recognition, comparing images taken from bodycams with a local list of people who should be approached with caution.[194]

Notably, this local list, developed through a communication network called Tec4se, is established by combining data from governmental authorities, emergency services such as fire and ambulance services, previous camera records, and local authorities, raising questions about precise grounds for inclusion in this list.[195]

Additionally, cloud-based systems have been trialed for the purpose of giving police on the street real-time access to large facial recognition databases.[196]

Finally, a few years back, the manager of the Dutch police unit focused on developing biometric data surveillance technologies stated that he was conducting a trial using facial recognition technology developed by French law enforcement, which had the ability to identify people in videos of large crowds.[197]

However, our research efforts have shown that the precise content of these trials is often unclear and it is difficult to ascertain their precise details, grounds, and safeguards. Nevertheless, it is clear that these trials will continue, with the Dutch Minister for Justice and Security stating in November 2019 that he was open to the Dutch police carrying out further experiments and trials to increase their use of facial recognition technology.[198]

#### 1.1.1.1 CATCH - Legal Analysis

Dutch police processing of data for the purpose of detecting and prosecuting crime falls outside of the scope of the GDPR. It is regulated by the Wet politiegegevens (Wpg) and Wetboek van Strafvorderingen (Sv) domestically and by the Data Protection Law Enforcement Directive (LED) at the EU level.[199]

Under the Wpg, if the Dutch police wish to process biometric data for the purpose of the unique identification of a person, they are only authorised to do so if it is 'unavoidable', a term appearing similar to strict necessity, and the data is sufficiently protected.[200] Similarly, under the LED, biometric data can only be processed if strictly necessary, to protect the vital interests of the data subject or of another natural person and with appropriate safeguards in place.[201]

It is questionable whether the grounds of strict necessity and/or unavoidability apply to the use of CATCH. Statistics released by the Dutch police have shown that only around 10% of usages of CATCH lead to a potential match, and, even in cases of a match, it is unclear whether this was useful to the investigation or actually led to a conviction.[202] Given its low rate of success, the CATCH system has not proved to be necessary to prosecuting crimes in the vast majority of cases.

---

186 **Niels Waarlo en Laurens Verhagen, 'De stand van gezichtsherkenning in Nederland' de Volkskrant (2020) available at:** https://www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028

187 **Tweede Kamer der Staten-Generaal, Kamerstuk 32761 nr. 152: Verwerking en bescherming persoonsgegevens - Brief van de Minister van Justitie en Veiligheid (25th of November 2019), available at:** https://zoek.officielebekendmakingen.nl/kst-32761-152.html

188 **RTL Nieuws, 'Gezichtsherkenning in de openbare ruimte: moeten we daar blij mee zijn?' RTL (2020) available at:** https://www.rtlnieuws.nl/nieuws/nederland/artikel/4997021/gezichtsherkenning-openbare-ruimte-bits-freedom-digitaal-online

189 **Ibid.**

190 **Waarlo and Verhagen,** de Volkskrant (2020).

191 **Statline, 'Geregistreerde criminaliteit; soort misdrijf, regio' Opendata CBS (2021) available at:** https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?fromstatweb

192 **Waarlo and Verhagen,** de Volkskrant (2020).

193 **Elsbeth Stoker,** de Volkskrant (2016).

194 **Wester van Gaal,** VICE (2019).

195 **Regio Twente, 'Nieuw communicatienetwerk Tec4se ondersteunt veiligheids- en hulpverleningsdiensten bij inzet' Nieuws (2014) available at:** https://www.regiotwente.nl/over-regio-twente/pers-en-media/nieuws/731-nieuw-communicatienetwerk-tec4se-ondersteunt-veiligheids-en-hulpverleningsdiensten-bij-inzet

196 **Ibid.**

197 **Reinier Kist, 'Politiesoftware scant gezichten van verdachten' NRC (2018) available at:** https://www.nrc.nl/nieuws/2018/02/19/politiesoftware-scant-gezichten-van-verdachten-a1592781#:~:text=De%20software%2C%20genaamd%20'CATCH',identiteit%20van%20een%20misdadiger%20op

198 **Tweede Kamer der Staten-Generaal, Kamerstuk 32761 nr. 152: Verwerking en bescherming persoonsgegevens - Brief van de Minister van Justitie en Veiligheid (25th of November 2019), available at:** https://zoek.officielebekendmakingen.nl/kst-32761-152.html

The size of the criminal justice database linked to CATCH increases the risk of inaccuracies, further casting doubt on whether it can be useful to the prosecution of crime. Indeed, previous uses of mass facial recognition technology by police in other countries saw 81% of 'suspects' wrongly identified and had error rates of up to 100%.[203]

Research has also revealed that algorithms can be biased, demonstrating that facial recognition systems have higher error rates in identifying black faces and female faces.[204]

Finally, in a recent criminal case in the Netherlands, the prosecution sought to convict a defendant of theft, money laundering, and membership of a criminal organisation solely on the basis of a 'match' with security footage identified through CATCH.[205]

Notably, the defendant was acquitted, with the court of Zeeland-West-Brabant ruling that there was not enough evidence to support a conviction.[206] If this case sets a precedent, it is unclear how police will be able to use CATCH-based identification as a ground of evidence in criminal cases where no other evidence exists, further undermining the contribution of the system to the prosecution of crime and, accordingly, its necessity.

Furthermore, not enough safeguards are in place to ensure that CATCH functions correctly and accurately.

A recent investigation revealed that the Dutch police failed to carry out a Data Protection Impact Assessment of CATCH before it came into force.[207]

While, at the time, this was not required by law, the clear failure by the Dutch police to consider the privacy risks associated with the CATCH system has significantly increased the risk of the data used in it being insufficiently protected. As detailed above, the Dutch police claim that safeguards are in place by way of two so-called, and undisclosed, "human experts" (with no transparency as to their purported "expertise" or how "expertise" is assessed in the circumstances), who are said to "verify potential matches".[208]

However, there is no accountability nor transparency within this purported check and balance, as the identities and fields of so-called "expertise" of the so-called "human experts" are kept secret.

Importantly, research has shown that human operators who assess facial recognition matches often defer to the algorithm's decisions, a phenomenon which is called 'automation bias'.[209]

Considering the grave risks posed by police use of facial recognition surveillance technology, such as its potential to discourage the use of public spaces and its ability to have a chilling effect on freedom of speech, freedom of association, and freedom of peaceful assembly, these safeguards cannot be sufficient to justify the disproportionate interference, invasion, and intrusion with privacy rights and other fundamental, universally recognised rights (detailed above) caused by CATCH.[210]

Another concern raised by CATCH is the Dutch police's proven inability to remove those who had been acquitted of crimes from the system.[211]

Under the Wpg, distinctions between different categories of people must be made as much as possible, such as between suspects, victims, and convicts.[212]

Within the CATCH criminal justice database, no distinction is made between suspects and convicts.[213] Even though this legal obligation is qualified by the requirement to make this distinction 'as much as possible',[214] the fact that those acquitted of crimes are usually not removed from the database even when they should be by law casts serious doubt on whether the Dutch police are fulfilling this obligation to the best of their abilities.

---

199 **Wet politiegegevens available at: https://wetten.overheid.nl/BWBR0022463/2020-01-01; Wetboek van Strafvordering available at:** https://wetten.overheid.nl/BWBR0001903/2021-01-01; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

200 **Wet politiegegevens,** Article 5.

201 **Law Enforcement Directive,** Article 10.

202 **RTL Nieuws,** RTL (2020).

203 **David Davis, 'Facial recognition technology threatens to end all individual privacy' The Guardian (2019) available at:** https://www.theguardian.com/commentisfree/2019/sep/20/facial-recognition-technology-privacy

204 **Priyanka Boghani, 'Artificial Intelligence Can Be Biased. Here's What You Should Know.' Frontline (2019) available at:** https://www.pbs.org/wgbh/frontline/article/artificial-intelligence-algorithmic-bias-what-you-should-know

205 **Rechtbank Zeeland-West-Brabant, Decision ECLI:NL:RBZWB:2019:2191 (17th of May 2019), available at:** https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBZWB:2019:2191

206 **Ibid.**

207 **Stan Hulsen,** Nu.nl (2021).

208 **Waarlo and Verhagen,** de Volkskrant (2020).

209 **European Digital Rights, Ban Biometric Mass Surveillance (Brussels 2020), available at:** https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf, p. 29.

210 **European Digital Rights, 'Your face rings a bell: Three common uses of facial recognition' Resources (2020) available at:** https://edri.org/our-work/your-face-rings-a-bell-three-common-uses-of-facial-recognition

Furthermore, under the Sv, police are only authorized to take pictures of suspects who are suspected of having committed a crime for which they can be held in pre-trial detention.[215] However, this legal provision was only introduced in 2010; before then, pictures could be taken without this requirement focused on the gravity of the potential crime.[216] Nevertheless, police are using pictures taken before 2010 when applying CATCH, raising further questions about the legality of its use under domestic law, considering that these pictures do not conform with current legal requirements.[217]

Finally, the large number of facial recognition surveillance technology "trials" currently being carried out by the Dutch police raises concerns of general democratic transparency and accountability.

Generally, information about these "trials", the data they collect, and their legal basis is unavailable to the public and, in the experience of the authors, significantly difficult to access.This lack of information makes it difficult to have independent oversight, accountability, and, ultimately, public confidence in these deployments and removes any possibility of a public debate on their desirability.

Even if these deployments are 'only' trials, there is no information on the temporal implementation of them, or even basic general information about their nature, operations, implementation, and end-date.

Furthermore, the use of the terminology of "trials" cannot serve as an excuse to escape the legal obligations imposed by EU data protection law, as emphasised by the Swedish data protection authority in a landmark case where it deemed a small-scale trial involving facial recognition surveillance technology in a school to be illegal.[218]

While this case only concerned Sweden, it sets an important comparative precedent which can hopefully inform judicial reasoning on facial recognition surveillance technology across Europe.

### 1.1.2. Foreign National Database

In addition to the expansive and ever-growing criminal justice database of the Netherlands, a so-called "Foreign National Database" exists which contains pictures of around 7 million people, whose inclusion is based solely on their lack of Dutch nationality, upon which CATCH facial recognition technology can be applied.[219] However, more stringent limits are placed on the use of this database. It can only be used following an order by an authorised officer of justice.[220]

A judge-commissioner must also give permission for it to be used and must scrutinise the reasons given for this use.[221] The system can be used to identify foreign nationals, but also to identify suspects of crimes if there is reasonable suspicion that the suspect is a foreign national.[222]

Furthermore, it can be used if an investigation has allegedly reached a 'dead end', so that the use of the system would then be justified as being in the (public) interest of the investigation.[223]
For example, this would be the case if there is a certain urgency to identify the person who has committed the crime. However, the crime must be of a sufficiently serious nature that pre-trial detention is permitted.[224]

#### 1.1.2.1 Foreign National Database - Legal Analysis

While police use of CATCH primarily for criminal justice purposes is regulated by the Wpg and the LED, these do not apply to police functions of border control and enforcement of immigration law, and correspondingly, the so-called "Foreign Nationals Database" used by Dutch Police.[225]

Instead, the Foreign National Database and the application of CATCH to it are regulated by the Wet Biometrie Vreemdelingenketen (Wbvk) within the Vreemdelingenwet 2000 and by the GDPR on a European level.[226]

Domestically, the Wbvk authorises the collection and processing of the biometric data of foreign nationals, purportedly for the purpose of addressing identity and document fraud.[227] Because of the Wbvk's far-reaching infringement on privacy protections, it automatically expires seven (7) years after coming into force, the next automatic expiry date being in 2021.[228]

Accordingly, the Dutch Government has proposed to extend this law by another five (5) years.[229] However, in response to this, the Dutch DPA recently issued an official recommendation in which it is critical of the Wbvk and the proposal to extend it, holding that the privacy of foreign nationals is insufficiently protected by it.[230]

---

211 **Stan Hulsen,** Nu.nl (2021).
212 **Wet politiegegevens,** Article 6b.
213 **Stan Hulsen,** Nu.nl (2021).
214 **Wet politiegegevens,** Article 6b.
215 **Wetboek van Strafvordering,** article 55c(2).
216 **Lotte Houwing, 'Minister komt met zorgwekkende antwoorden op Kamervragen over CATCH' Bits of Freedom (2019) available at:** https://www.bitsoffreedom.nl/2019/09/11/minister-komt-met-zorgwekkende-antwoorden-op-kamervragen-over-catch
217 **Ibid.**
218 **Sofie Edvardsen, 'How to interpret Sweden's first GDPR fine on facial recognition in school' IAPP (2019) available at:** https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school
219 **Waarlo and Verhagen,** de Volkskrant (2020).
220 **RTL Nieuws,** RTL (2020).
221 **Ibid.**
222 **Tweede Kamer der Staten-Generaal, Kamerstuk 32761 nr. 152: Verwerking en bescherming persoonsgegevens - Brief van de Minister van Justitie en Veiligheid (25th of November 2019),** available at: https://zoek.officielebekendmakingen.nl/kst-32761-152.html
223 **Ibid.**
224 **Ibid.**
225 **Autoriteit Persoonsgegevens, 'Politie' Politie en Justitie (2021) available at:** https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/politie
226 **Vreemdelingenwet, available at:** https://wetten.overheid.nl/BWBR0011823/2021-02-20

The DPA/AP held that two past evaluations of the Wbvk have shown that the necessity of collecting biometric data of foreign nationals has been insufficiently demonstrated and that this practice is not proportionate.[231]

In particular, it is unclear why the collection of data cannot be limited to specific categories of foreign nationals; it is hard to remove the data once it is registered in the database; and the role of facial recognition surveillance within this legal framework is unclear, as facial images are not specifically mentioned within the Dutch law, unlike fingerprints.[232]

Given that the Wbvk does not provide for the proportionate processing of the biometric data of foreign nationals under domestic law, it is important to examine how the Dutch Foreign National Database holds up under European law, in particular the GDPR. Under the GDPR and the Dutch UAVG implementing it, the processing of special categories of personal data, including biometric data, is prohibited unless explicit consent has been obtained, or for authentication or security reasons for the purpose of 'a grave public interest'.[233]

The DPA/AP has stated that a grave public interest would for example be the protection of a nuclear power plant.[234] Given the clear power imbalance between police and foreign nationals, the first ground cannot be satisfied.

However, considering the second ground, the Dutch Council of State upheld the practice in a recent case, ruling that the collection of fingerprints and facial images of foreign nationals was necessary to prevent identity and document fraud.[235]

Nevertheless, despite this apparent necessity, which is disputed by the Dutch DPA in any case, the sheer size of the database increases the risk of breaches of fundamental rights. This size increases the risk of mistakes and inaccuracies, further exacerbated by the fact that the database solely includes the biometric data of foreign nationals.

Research has convincingly demonstrated that facial recognition technology and its algorithms are often biased and inaccurate at identifying groups such as racial minorities and a person's face can be a marker of protected characteristics

---

227 **Autoriteit Persoonsgegevens, 'AP adviseert kritisch over verwerken biometrische gegevens vreemdelingen' Nieuws (2020) available at:** https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-adviseert-kritisch-over-verwerken-biometrische-gegevens-vreemdelingen

228 **Ibid.**

229 **Autoriteit Persoonsgegevens,** Nieuws (2020).

230 **Autoriteit Persoonsgegevens, Recommendation z2020-01329: Advies over het concept voor Wijziging van de Vreemdelingenwet 2000 ter bestendiging van verwerking biometrie (24th of June 2020), available at:** https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_biometrische_gegevens_vreemdelingen.pdf

such as religion, raising concerns of discrimination and social biases being reflected within the technology itself.[236]

Considering the fact that the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance noted in 2020 that racial and ethnic profiling appears to be a persistent practice among Dutch police, their access to this Foreign National Database is deeply concerning.[237]

In short, the collection of the biometric data of foreign nationals and the application of facial recognition technology to it, despite the inclusion of more stringent safeguards than the ordinary CATCH system, create a disproportionate, unnecessary, and potentially discriminatory interference with the fundamental rights of foreign nationals, a view supported by the Dutch data protection authority.

### 1.1.3 Clearview AI

There are allegations that Dutch public authorities use the controversial Clearview AI facial recognition system, a facial recognition app developed by American technology company Clearview AI, which allows users to upload a picture of a person to find public pictures of that person and where they appear.[238]

The Clearview AI system contains a database of more than three billion images, derived from Facebook, YouTube, and other websites largely without the knowledge of those individuals in the images.[239]

The allegations of the use of Clearview AI by Dutch police and public authorities come from a 2020 Buzzfeed investigation which found the Dutch government to be one of the customers of Clearview AI, although it is unclear which part of the Dutch government uses this.[240]

---

231 **Ibid.**

232 **Autoriteit Persoonsgegevens, Recommendation z2020-01329** (20th of June 2020).

233 **GDPR,** Article 9; UAVG, Article 22.

234 **Autoriteit Persoonsgegevens, 'AP: Pas op met camera's met gezichtsherkenning' Nieuws (2020) available at:** https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-pas-op-met-camera%E2%80%99s-met-gezichtsherkenning

235 **Raad van State, Uitspraak 201601536/3/V3 en 201601554/3/V3 (Reference ECLI:NL:RVS:2020:1168; 29th of April 2020), available at:** https://www.raadvanstate.nl/actueel/nieuws/@120973/201601536-3-v3-en-201601554-3-v3

236 **European Digital Rights, 'Facial recognition and fundamental rights 101' Resources (2019) available at:** https://edri.org/our-work/facial-recognition-and-fundamental-rights-101**; Tom Simonite, 'Photo Algorithms ID White Men Fine—Black Women, Not So Much' Wired (2018) available at:** https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much

237 **Human Rights Council, Visit to The Netherlands: Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance** (2 July 2020), UN Doc A/HRC/44/57/Add.2, para. 50.

The Dutch government denies that the Dutch police use this technology and the details remain unclear and unaccountable.[241] Furthermore, linking the Clearview AI database to the abovementioned CATCH system would give the police access to an unprecedented amount of biometric data.

#### 1.1.3.1 Clearview AI - Legal Analysis

The potential deployment of Clearview AI by Dutch police and the ambiguity surrounding its use by Dutch public authorities raise particular concerns of transparency.

The LED at Preamble 26 states that personal data must be processed in a transparent manner, highlighting the importance of transparency in all processing of personal data. Indeed, a key concern in the area of biometrics is that their deployment is often shrouded in secrecy and deliberately hidden from the public, even though transparency is key to creating public awareness of the use of these technologies and the enforcement of existing legislation.[242]

If the Dutch government has indeed used Clearview AI, as the 2020 Buzzfeed investigation alleges, it must be transparent about the government organs which have used the technology, on whom it has been used, for what purpose, and the legal basis for this.

Furthermore, given the far-reaching nature of Clearview AI and its potential for mass biometric surveillance, a transparent account of how the data is being used would likely confirm its illegality and breach of many of the human rights mentioned above.

### 1.1.4 Camera in Beeld

In 2016, the Dutch police introduced a database called 'Camera in Beeld', where private citizens and businesses who own security cameras can register their security camera for police access in controlling crime, for free through a simple online form.[243]

If a crime has been committed near a registered camera, the police are able to access the camera footage, with the intention to speed up the investigation and the apprehension of suspects.[244]

Around 228,530 cameras have been registered under the Camera in Beeld scheme as of December 2019.[245] Police strongly encourage camera owners to register their camera in this database, for example by allowing them to sign up for a 'free scan' to examine the quality of their security cameras. In signing up for this scan, the user's camera is automatically registered with Camera in Beeld. [246]

This approach by Dutch police preys on the social peer pressure of "nothing to hide", which encourages citizens to not only consent to, but actively participate in, the intrusion of their own and others' privacy rights for the convenience of the State and its law enforcement agencies.

Even though the Dutch police do provide some guidance to camera owners to ensure that the cameras do not infringe upon privacy rights, they paradoxically also tell camera owners that cameras are allowed to be placed in a location where it is inevitable that part of public space is filmed.[247]

They have also explicitly reassured users that they should not be afraid of being caught violating data protection laws if they register for Camera in Beeld, as Camera in Beeld is "not intended to enforce data protection and privacy laws".[248]

Accordingly, an investigation found that 87.6% of cameras registered under Camera in Beeld film public space at least partially.[249] Although the images from these cameras are not used for real-time facial recognition, as mentioned in section 1.1.1, the Dutch police use a system of facial recognition technology called CATCH.

The Dutch police apply CATCH to a wide variety of images, including footage recorded by security cameras registered under Camera in Beeld.[250]

This in turn allows the police to make comparisons between images from registered security cameras and images from its criminal justice database using CATCH, demonstrating how Camera in Beeld can indirectly lead to uses of biometric data which could be considered mass surveillance.

Furthermore, the Dutch police can order owners of cameras registered under Camera in Beeld to provide them with images from their security cameras by law and even charge owners with a crime and jail time if they do not comply.[251]

### 1.1.5. Smart doorbells

So-called "smart doorbells" are being increasingly used in the Netherlands.[252] Around 16% of Dutch households use smart doorbells, usually produced by Ring (Amazon), Google Nest, or Skybell.[253]

While smart doorbells can be purchased privately by households, various public authorities and municipalities have recently encouraged the use of smart doorbells as well as their registration in the Camera in Beeld database mentioned in section 2.1.4.

For instance, the Dutch Ministry for Security and Justice has subsidised various municipalities to distribute Ring doorbells to inhabitants for free through a project called 'Slimme Deurbel', especially in areas with a high rate of burglaries.[254]

This project is currently running in at least four municipalities (Almere, Nissewaard, Eindhoven, Den Haag) and around 360 smart doorbells have been distributed which have been automatically registered with Camera in Beeld.[255]

Other municipalities which appear to be using smart doorbell trials include, for example, Gouda, where inhabitants receive a €250 subsidy if they buy a smart doorbell and register it with Camera in Beeld.[256]

The registration of smart doorbells in the Camera in Beeld database raises the above mentioned potential of applying CATCH facial recognition technology to the images registered by the smart doorbells and the corresponding use of biometric data in ways that could lead to mass surveillance. Notably, in terms of effectiveness, the use of smart doorbells to prevent crime has mixed results. Research has shown that, while participants feel safer when using smart doorbells, actual crime figures barely decrease.[257]

In Almere, one of the municipalities where smart doorbells are being used, crime on a street-by-street level appeared to have decreased after smart doorbells were introduced, with burglaries significantly going down.[258] However, car burglaries increased and burglaries in a control neighbourhood which did not have smart doorbells went down at the same rate as those using the smart doorbells.

---

238 **Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' The New York Times (2020) available at:** https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

239 **Ibid.**

240 **Ryan Mac, Caroline Haskins and Logan McDonald, 'Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA' Buzzfeed News (2020) available at:** https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement

241 **NOS Nieuws, 'Ook in Nederland gezichtsherkenning met omstreden Programma Clearview' NOS (2020)** https://nos.nl/artikel/2324950-ook-in-nederland-gezichtsherkenning-met-omstreden-programma-clearview.html

242 **European Digital Rights, Ban Biometric Mass Surveillance (Brussels 2020), available at:** https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf, p. 38.

243 **Politie Nederland, 'Camera in Beeld' Thema's (2020) available at:** https://www.politie.nl/themas/camera-in-beeld.html?sid=07c1d5df-60bf-470a-993f-f9f212c9dd00

244 **Ibid.**

245 **Floris Poort, 'Al 229 duizend bewakingscamera's in Nederland' RTL Nieuws (2019) available at:** https://www.rtlnieuws.nl/tech/artikel/4957711/nederland-telt-228530-gemelde-bewakingscameras

246 **Politie Nederland, 'Tweehonderdduizend extra 'ogen' voor politie' Nieuws (2019) available at:** https://www.politie.nl/nieuws/2019/januari/10/tweehonderdduizend-extra-%E2%80%98ogen%E2%80%99-voor-politie.html

247 **Politie Nederland,** Thema's (2020).

248 **Lotte Houwing, 'In beeld van een buitenwettelijk surveillancenetwerk' Joop (2019) available at:** https://joop.bnnvara.nl/opinies/in-beeld-van-een-buitenwettelijk-surveillancenetwerk; **Redactie, 'Veel huiseigenaren melden zich aan voor Camera in Beeld' Beveiligingsnieuws (2019) available at:** https://beveiligingnieuws.nl/nieuws/veel-huiseigenaren-melden-zich-aan-voor-camera-in-beeld

249 **Daan van Monsjou, 'Bijna 9 op de 10 geregistreerde beveiligingscamera's filmen openbare weg' Tweakers (2019) available at:** https://tweakers.net/nieuws/161164/bijna-9-op-de-10-geregistreerde-beveiligingscameras-filmen-openbare-weg.html

Furthermore, Dutch police only requested images from smart doorbells twelve times throughout the trial. In ten of these cases, no recognisable faces were recorded by the doorbell, and, in two of the cases, the images from the doorbell led to further investigations but did not lead to convictions.

The Dutch police have used these limited and mixed results to encourage other municipalities and their inhabitants to buy smart doorbells, using a misleading headline 'Digital doorbells makes the streets safer' even when there is no empirical and unqualified proof for this.[259]

250 **Lotte Houwing, 'Hoe de politie haar buitenwettelijke surveillancenetwerk uitbreidt' Bits of Freedom (2020) available at:** https://www.bitsoffreedom.nl/2020/02/05/hoe-de-politie-haar-buitenwettelijke-surveillancenetwerk-uitbreidt

251 **Lotte Houwing,** Joop (2019).

252 **Katja Mur, 'Careful of privacy violations when installing camera doorbells, privacy watchdog warns' NL Times (2020) available at:** https://nltimes.nl/2020/10/06/careful-privacy-violations-installing-camera-doorbells-privacy-watchdog-warns

253 **Rudy Bouma and Fleur Damen, 'Slimme deurbel rukt op in strijd tegen inbraken, maar hoe zit het met privacy?' NOS (2020) available at:** https://nos.nl/nieuwsuur/artikel/2318362-slimme-deurbel-rukt-op-in-strijd-tegen-inbraken-maar-hoe-zit-het-met-privacy.html

254 **Bourma and Damen,** NOS (2020).

255 **Tijs Hofmans, 'Gratis deurbellen tegen criminaliteit: Het twijfelachtige effect en de privacyzorgen' Tweakers (2019) available at:** https://tweakers.net/reviews/7524/all/digitale-deurbellen-het-twijfelachtige-effect-en-de-privacyzorgen.html

256 **Julian Huijbregts, 'Gouda geeft subsidie voor camera of videodeurbel bij aanmelden politiedatabase' Tweakers (2019) available at:** https://tweakers.net/nieuws/160772/gouda-geeft-subsidie-voor-camera-of-videodeurbel-bij-aanmelden-politiedatabase.html

257 **Hofmans,** Tweakers (2019).

258 **Gemeente Almere, Evaluatie pilot digitale deurbel Almere 2018 (Almere 2018) available at:** https://veilig.almere.nl/fileadmin/files/almere/beeldbank/veiligheid/Evaluatierapport_digi_deurbel_20190325_def.pdf

259 **Rijksoverheid, 'Digitale deurbel maakt de straten veiliger' Nieuws (2019) available at:** https://www.rijksoverheid.nl/actueel/nieuws/2019/03/28/digitale-deurbel-maakt-straten-veiliger

#### 1.1.5.1 Camera in Beeld and Smart Doorbells - Legal Analysis

When the Dutch police use camera footage from cameras and smart doorbells registered under Camera in Beeld and apply facial recognition surveillance technology to it using CATCH, their actions are regulated by the Wpg and LED, raising the legal concerns mentioned in section 1.1.1.1.

However, these cameras and smart doorbells, in their initial use without police involvement, concern a private form of data collection and are therefore regulated by the GDPR. Because facial recognition surveillance technology has not yet been applied to them, these cameras concern ordinary personal data, rather than the special category of biometric data, and are thus regulated by Article 6 of the GDPR.

Indeed, this is precisely why Camera in Beeld is so attractive to the Dutch police: normally, police must receive permission from mayors to install facial recognition cameras, a requirement which can be handily avoided by this private network.[260]

Nevertheless, most of these smart doorbell cameras likely do not fulfill the requirements of data protection laws. Pursuant to Dutch data protection laws, it is prohibited to film public space unless there is a direct threat or reason for this, or if filming part of public space is inevitable due to the characteristics of the property.[261]

However, an investigation found that over 87% of cameras registered with Camera in Beeld film public space, so it is questionable whether this was inevitable or had a direct reason in each of these cases.[262]

Similarly, referring to smart doorbells specifically, the DPA/AP has stated that they are likely to be illegal under data protection law given their tendency to film public space.[263] The use of these doorbells can also not be justified by their effectiveness, with no evidence of a positive impact on crime prevention existing thus far, meaning that the breach of privacy posed by this technology is not proportionate to its purpose of crime reduction.[264]

---

260 **Lotte Houwing, 'Hoe de politie haar buitenwettelijke surveillancenetwerk uitbreidt' Bits of Freedom (2020) available at:** https://www.bitsoffreedom.nl/2020/02/05/hoe-de-politie-haar-buitenwettelijke-surveillancenetwerk-uitbreidt

261 **Autoriteit Persoonsgegevens, 'Camera's bij huis en bij de buren' Foto en Film (2021) available at:** https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/cameras-bij-huis-en-bij-de-buren

262 **van Monsjou,** Tweakers (2019).

263 **Rudy Bouma and Fleur Damen, 'Slimme deurbel rukt op in strijd tegen inbraken, maar hoe zit het met privacy?' NOS (2020) available at:** https://nos.nl/nieuwsuur/artikel/2318362-slimme-deurbel-rukt-op-in-strijd-tegen-inbraken-maar-hoe-zit-het-met-privacy.html

264 **Hofmans,** Tweakers (2019).

Finally, smart doorbells in particular have been characterised by a lack of safeguards, with data from Ring (Amazon) doorbells being stored on American servers and recently falling victim to a data breach by hackers where the data of 3,600 users was leaked onto the darknet.[265]

Despite this apparent illegality, the network of cameras and doorbells registered through Camera in Beeld is so vast that the DPA/AP does not have the capacity to control it or enforce data protection laws on it, creating a trend of impunity despite the grave threats to privacy posed by these systems.[266] Furthermore, trials with cameras or smart doorbells are run in a decentralised way by municipalities, with no central oversight over where and in what way data is being collected, raising further concerns of transparency and impunity.[267]

Even without directly using biometric data, private use of these cameras and smart doorbells has the potential to violate data protection laws, and it is therefore worrying that police and local authorities actively encourage the use of these forms of surveillance through various means.[268]

What's more, this potential breach is exacerbated by the constant possibility of the police accessing footage from these cameras and applying facial recognition technology to it, raising further privacy and legal concerns.

265 **Bouma and Damen,** NOS (2020).

266 **BNR Webredactie, 'Forse Toename Cameras met Gezichtsherkenning, Capaciteit AP Schiet Tekort' BNR (23 November 2020) available at:** https://www.bnr.nl/nieuws/juridisch/10426941/forse-toename-camera-s-met-gezichtsherkenning

267 **Tijs Hofmans, 'Gratis deurbellen tegen criminaliteit: Het twijfelachtige effect en de privacyzorgen' Tweakers (2019) available at:** https://tweakers.net/reviews/7524/all/digitale-deurbellen-het-twijfelachtige-effect-en-de-privacyzorgen.html

268 **For instance,** Huijbregts, Tweakers (2019).

## 1.2 Municipalities

In a survey of municipalities in the Netherlands carried out by Volkskrant, there was a general consensus against the use of facial recognition surveillance technology, even when some local authorities are showing interest in it.[269] However, certain municipalities do use facial recognition technology for large events, as a purported means of crowd control and preventing crime and public disturbances.

For instance, facial recognition surveillance technology was used during a carnival in Den Bosch in 2019.[270] The organisers used real-time facial recognition surveillance technology to identify everyone entering the street on which the carnival was held, including those in costume.

No less than 11,381 faces were identified as they entered the carnival street and were compared with the faces of those who had misbehaved during a previous carnival or who had a ban (although it is unclear whether this alleged 'misbehaviour' was actually proven through a judicial process).

Using the technology, developers identified less than 10 people who had bans, thereby calling the proportionality of the programme into question.[271] Despite these issues, the same technology is being used during large events in the Netherlands, including Liberation Day in Wageningen, Decibel Festival, and carnival in Oeteldonk.[272]

A further use of facial recognition surveillance technology by a municipality is an identity fraud test used in Zwolle and Midden-Delfland, where facial recognition surveillance technology is applied when residents request new identity documents to verify their identity.[273] The data is said to be encrypted and is required to be deleted after 3 months.[274]

269 **Waarlo and Verhagen,** de Volkskrant (2020).
270 **Bart Gotink,** BD (2019).
271 **Ibid.**
272 **Crowdwatch Nederland, various Facebook posts:** https://www.facebook.com/crowdwatchnl/posts/1547482191928815 (2017), https://www.facebook.com/crowdwatchnl/posts/1664213833588983 (2017), https://www.facebook.com/crowdwatchnl/posts/2385899338087092 (2019).
273 **Francisca Muller, 'Echt of nep? In Zwolle hebben ze identiteitsfraude sneller door' DS (2018)** https://www.destentor.nl/zwolle/echt-of-nep-in-zwolle-hebben-ze-identiteitsfraude-sneller-door~ad2273f5/?referrer=https%3A%2F%2Fwww.google.com%2F
274 **Ibid.**

## 1.2 Municipalities - Legal Analysis

The collection and processing of biometric data by municipalities in the Netherlands is governed by the Wet Basisregistratie Personen (WBP) domestically and by the GDPR at a European level. Under domestic law, the WBP authorises specific forms of data collection and data sharing by municipalities, allowing them to register the personal data of inhabitants such as name, gender, and date of birth in a central database, which can be passed on to various government departments.[275]

Notably, the WBP does not concern biometric data, meaning that the legal basis for the collection of biometric data by municipalities must be found in the GDPR instead. As discussed previously, the processing of special categories of personal data is prohibited under the GDPR and UAVG, unless either (1) the person whose data is being processed has explicitly consented to it or (2) the data is collected for security or authentication reasons for the purpose of a *'grave public interest'*, such as the protection of a nuclear power plant.[276]

Regarding the use of facial recognition by municipalities during large events, participants had no opportunity to explicitly consent to the collection of their biometric data, with their face being scanned automatically upon entry.[277] Even if participants were made aware of the technology being used, it is widely recognised that silence cannot be interpreted as acquiescence and consent must be explicitly given.[278]

Accordingly, the first exception cannot apply here. Considering the second exception, the users of facial recognition technology during the carnival admit that its deployment was a 'luxury' and only ten people with bans were identified.[279]

Evidently, the use of this technology was not necessary for public security during the carnival. This is also recognised by the DPA/AP, which states that municipalities can only use camera surveillance if less intrusive measures are not sufficient for enforcing law and order, failing the second exception.[280]

---

275 **Autoriteit Persoonsgegevens, 'Basisregistratie Personen (BRP)' Overheid (2021) available at:** https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/overheid/basisregistratie-personen-brp

276 **GPDR, Article 9; UAVG, Article 22; Autoriteit Persoonsgegevens,** Nieuws (2020).

277 **Bart Gotink,** BD (2019).

278 **Autoriteit Persoonsgegevens, 'Biometrie' Identificatie (2021) available at:** https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/biometrie#faq

279 **Bart Gotink,** BD (2019).

Regarding the use of facial recognition surveillance technology to verify inhabitants' identity when requesting new identity documents, it is clear that inhabitants have no choice but to consent when requesting essential identity documents, putting into question the extent to which consent can be freely given.

Regarding the second exception, while preventing fraud is a justifiable security reason, less intrusive measures could again be used and have been used for years by municipalities around the country, such as a simple human comparison of the image on the identity document and the person. This further casts doubt on the necessity of the use of facial recognition technology in this case.

Clearly then, given that these forms of biometric data collection have no legal basis under the WBP and GDPR, these deployments of biometric surveillance technologies by municipalities are likely to be illegal under data protection law, constituting a grave breach of privacy and other fundamental universally recognised rights.

Furthermore, the Dutch Constitution requires that any infringement upon the right to privacy must have a sufficiently precise legal basis.

Accordingly, even if the use of biometric surveillance by municipalities is sporadic and not yet widespread, the lack of legal basis for their use also touches upon Dutch constitutional rights.

Clearly then, given that these forms of biometric data collection have no legal basis under the WBP and GDPR, these deployments of biometric surveillance technologies by municipalities are likely to be illegal under data protection law, constituting a grave breach of privacy and other fundamental universally recognised rights. Furthermore, the Dutch Constitution requires that any infringement upon the right to privacy must have a sufficiently precise legal basis.[281]

Accordingly, even if the use of biometric surveillance by municipalities is sporadic and not yet widespread, the lack of legal basis for their use also touches upon Dutch constitutional rights.

---

280 **Autoriteit Persoonsgegevens, 'Cameratoezicht op openbare plaatsen' Foto en Film (2021) available at:** https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/cameratoezicht-op-openbare-plaatsen#onder-welke-voorwaarden-mag-een-gemeente-cameratoezicht-inzetten-7758

281 **Dutch Constitution, Article 10; de Rechtspraak, 'Belastingdienst mag foto's snelwegcamera's niet gebruiken' Nieuws (2017) available at:** https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Hoge-Raad-der-Nederlanden/Nieuws/Paginas/Belastingdienst-mag-fotos-snelwegcameras-niet-gebruiken.aspx

## 1.3 Conclusion

In conclusion, the use of biometric data surveillance technologies by public authorities in the Netherlands, such as the police and other local authorities and municipalities, generally result in a disproportionate infringement with privacy and data protections under Dutch domestic law, European law, and international human rights law, unable to be justified by reasons of necessity, legitimacy, or proportionality.

Furthermore, given their far-reaching implications, these deployments of biometric mass surveillance technologies by public authorities result in grave breaches of numerous fundamental and universally recognised human rights, both in the Dutch constitution, European law, and international law, including, but not limited to, the following:

**1.** the universally recognised right to privacy,[282]
**2.** the European-wide recognised right to the protection of personal data,[283]
**3.** the universally recognised right to freedom of expression,[284]
**4.** the universally recognised right to freedom of thought, conscience, and religion,[285]
**5.** the universally recognised right to freedom of peaceful assembly,[286]
**6.** the universally recognised right to freedom of association,[287]
**7.** the universally recognised right to take part in public affairs,[288]
**8.** the universally recognised right to freedom of movement,[289]
**9.** inter alia.

The right to a private and family life, in particular, is recognised as a fundamental human right in constitutional and international law. This right is protected by a wealth of instruments, including the Dutch Constitution, the European Charter of Fundamental Rights, the European Convention on Human Rights, and the ICCPR, demonstrating its importance and underlining the human rights concerns these deployments raise.[290]

282 **ICCPR Art. 17,** UDHR Art. 12, ECHR Art. 8, EUChFR Art 7.
283 **EUChFR** Art. 8.
284 **ICCPR Art. 19,** UDHR Art. 19, ECHR Art. 10, EUChFR Art. 11.
285 **ICCPR Art. 18,** UDHR Art. 18, ECHR Art. 9, EUChFR Art. 10.
286 **ICCPR Art. 21,** UDHR Art. 20, ECHR Art. 11, EUChFR Art. 12.
287 **ICCPR Art. 22,** UDHR Art. 20, ECHR Art. 11, EUChFR Art. 12, International Labour Organization's Convention No. 87 on Freedom of Association and Protection of the Right to Organise.
288 **ICCPR Art. 25,** UDHR Art. 21, ECHR Art. 9, EUChFR Art. 39 and 40.
289 **ICCPR Art. 12,** UDHR Art. 13, ECHR Art. 2, EUChFR Art. 45.
290 **Dutch Constitution,** Article 10; European Charter of Fundamental Rights, Article 7; European Convention on Human Rights, Article 8; International Covenant on Civil and Political Rights, Article 17.

# 2. DEPLOYMENTS BY PRIVATE ENTITIES

## 2.1 Retail

**Private entities including retail stores, football clubs, stadiums, casinos, and many more use facial recognition technology with the intention to prevent crime and public disturbances.**

The use of biometric mass surveillance measures, particularly facial recognition, appear to be increasingly of interest in the private sector. Given the decentralised nature of these deployments and relatively low capacity of the Dutch AP, enforcement of data protection laws has been rather limited.

Certain retail stores in the Netherlands have been known to use facial recognition technology as a means of purportedly preventing shoplifting and crime, often attempting to identify customers with an alleged history of criminal behaviour at the entrance to prevent them from coming into the store.

A Jumbo store in Alphen Aan De Rijn - part of one of the most prominent Dutch supermarket chains - provides an example of this trend.[291] The store used facial recognition technology at its entrance to identify blacklisted customers who had previously been found shoplifting or who had a shopping ban.

The people identified were then prevented from coming into the store. This case received massive press coverage and negative attention, even going so far as to be part of an Urgent Question in the Dutch Second Chamber of Parliament.[292]

In response, the store's owner turned off the cameras in December 2019, pending a review by the Dutch Data Protection Authority.[293] The Dutch Data Protection Authority released a statement on the matter in December 2020, after the Jumbo store indicated its intention to turn the cameras back on.[294]

The AP unambiguously stated that the use of facial recognition technology in retail stores is disproportionate in cases where it is being used to prevent shoplifting.[295] Despite the illegality of the use of facial recognition technology in retail settings, several trials have been conducted using cameras for similar purposes, for example in Utrecht, although many of these have been suspended due to the high costs of the system and legal issues.[296]

## 2.2 Casinos

Several casinos have been using facial recognition technology for the same purposes of crime or nuisance prevention as police, retail stores, and municipalities. This technology is used to identify people with a ban from the casino, such as known gambling addicts. It uses a 'traffic light' system at the entrance which shows a green or red colour indicating whether the visitor can enter without problems.[297]

The Gambling House in Amsterdam is an example of this. They previously used a controversial system of facial recognition technology called Hikvision, which is partly owned by the Chinese government.

Allegations against this system claim that it supplies the same facial recognition technology that is used to oppress Uighur Muslims in China.[298] Because of this, Gambling House stopped using Hikvision.[299]

---

**291 Mitch van Helvert, 'Tientallen camera's houden klanten van filiaal Jumbo in the gaten: 'Willen we dit?" RTL Nieuws (2019) available at:** https://www.rtlnieuws.nl/nieuws/nederland/artikel/4941596/gezichtsherkenning-biometrie-alphen-jumbo-privacy

**292 Sander Dekker, 'Antwoord op vragen van het lid Verhoeven inzake het bericht 'Tientallen camera's houden klanten van filiaal Jumbo in de gaten: 'Willen we dit?"' Tweede Kamer der Staten-Generaal (2020) available at:** https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D01497&did=2020D01497

**293 Studio Alphen, 'Autoriteit Persoonsgegevens onderzoekt gezichtsherkenning bij supermarkt Jumbo' Studio Alphen Nieuws available at:** https://www.studioalphen.nl/nieuws/autoriteit-persoonsgegevens-onderzoekt-gezichtsherkenning-bij-supermarkt-jumbo

**294 Autoriteit Persoonsgegevens, 'Formele Waarschuwing AP aan supermarket om gezichtsherkenning' AP Nieuws (15 December 2020) available at:** https://autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning

They tried to replace it with another facial recognition system, but found that the alternatives were too expensive, so they decided to stop using facial recognition technology altogether.[300]

## 2.3 Football clubs and stadiums

Many football clubs use facial recognition technology for the purpose of safety, usually to recognise banned individuals and deny them access to their stadium.
An example of a system being used is 20Face Technology, a special turnstile equipped with facial recognition capabilities which football fans can use to enter the stadium. It is used by the football club Heracles.[301] The system is voluntary and the pictures are only saved on the fans' own smartphones, while the data is encrypted.[302]

However, the system does use artificial intelligence, which raises discrimination concerns, for example in terms of its application to people of differing races or ethnicities.[303]

Another example is the Johan Cruiff Arena in Amsterdam, which is trialling a 'digital perimeter', aimed at monitoring the area around the stadium using facial recognition. The intended purpose is making the area around the arena safer and contributing to improved mobility.[304]

295 **Autoriteit Persoonsgevens,** *AP Nieuws* (December 2020).
296 **Niels Waarlo en Laurens Verhagen, 'De stand van gezichtsherkenning in Nederland' de Volkskrant (2020) available at:** https://www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028/?referrer=https%3A%2F%2Fwww.google.com%2F
297 **Waarlo and Verhagen,** de *Volkskrant* (2020).
298 **Yuan Yang and Madhumita Murgia, 'Facial recognition: how China cornered the surveillance market' Financial Times (2019)** https://www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385
299 **Waarlo and Verhagen,** *de Volkskrant* (2020).
300 **Ibid.**

Other clubs use cameras which film the turnstiles and/or biometric cards with data encoded on them. The Johan Cruiff Arena is also using facial recognition technology for the purposes of employee registration and admitting people to events, as well as ordering food and drinks.

For the latter, customers can order food and drinks on an app, pay with their faces, and collect their order in the fast lane during the break.[305]

There have been recorded errors by facial recognition systems employed at football stadiums. One took place in the stadium of F.C. Den Bosch, which uses 24 "smart" cameras to film football fans at its turnstiles and compares the images with people filmed during reported incidents and people with stadium bans.[306]

A 20 year-old football fan who attended an event later received a letter from the football club giving him a temporary ban, claiming that he was involved in an incident where he violently confronted supporters and entered restricted areas.

This was incorrect, but the fan decided not to pursue it as he had no plans to enter the stadium again. He later got an email falsely claiming that he entered the stadium again despite the ban and received a €1000 fine on these grounds. He managed to contact the club and convince them that it was not him.

The club claimed that he had a similar posture and face to the person filmed, demonstrating the danger of using these types of technologies and the ease of making mistakes.[307]

---

301 **Gerben Kuitert, 'Heracles Almelo start proef met gezichstherkenning' Tubantia (2019) available at:** https://www.tubantia.nl/heracles/heracles-almelo-start-proef-met-gezichtsherkenning~ad9bd7e6

302 **Waarlo and Verhagen,** de *Volkskrant* (2020).

303 **Gerben Kuitert,** *Tubantia* (2019).

304 **Gemeente Amsterdam, 'Digitale Parameter' De Digitale Stad** https://www.amsterdam.nl/wonen-leefomgeving/innovatie/de-digitale-stad/digitale-perimeter

305 **Monique Evers, 'Margatens bedrijf verovert de Arena met gezichtsherkenning' De Limburger (2019) available at:** https://www.limburger.nl/cnt/dmf20190515_00105698

306 **Wim Heesterbeek, 'Camera's met gezichtsherkenning bij FC Den Bosch en in het casino: 'Dit kan niet zomaar" Omroep Brabant (2019) available at:** https://www.omroepbrabant.nl/nieuws/3003082/cameras-met-gezichtsherkenning-bij-fc-den-bosch-en-in-het-casino-dit-kan-niet-zomaar

307 **Ibid.**

## 2.4 Schipol Airport

Since 2008, the biggest airport in the Netherlands, Schiphol, has used facial recognition technology with the intention to make processes such as boarding smoother. E-gates at the airport compare the faces of EU citizen passengers with the picture on their identity documents in order to let them through.[308]

Schiphol airport is also trialing a biometric boarding system which scans a passenger's face, passport, and boarding pass and stores it, allowing the passenger to go document-free and use only their face as proof of identity and ticket.[309]

## 2.5 Public Transport

Facial recognition has been trialled by transport companies to identify those with public transport bans. A signal is usually sent to the driver if a banned individual is recognised by the cameras. The driver will then verify if the individual and the image match and act accordingly. These systems were initiated as a trial but it is unclear if they ever officially ended

For example, in Rotterdam, transport company RET started a facial recognition trial in 2010 using this system, sponsored in part by the Interior Ministry of the Netherlands.[310] While new trams have been phased in which do not use this facial recognition technology, the trial was never officially ended even though it was only intended to last for one year.[311]

308 **Waarlo and Verhagen**, de Volkskrant (2020).

309 **Schiphol, 'Schiphol launches pilot for boarding by means of facial recognition' Schiphol News (2019) available at:** https://news.schiphol.com/schiphol-launches-pilot-for-boarding-by-means-of-facial-recognition

310 **Brenno de Winter, 'RET voegt gezichtsherkenning toe aan camerabewaking' Nu.nl (2011) available at:** https://www.nu.nl/binnenland/2613144/ret-voegt-gezichtsherkenning-toe-camerabewaking.html

## 2.6 International Legal Framework

The deployments above appear to be incompatible with certain fundamental rights enumerated in the EU Charter of Fundamental Rights and the European Convention on Human Rights.

This incompatibility stems from the way these deployments indiscriminately treat all people as possible criminals - an approach that violates fundamental rights such as privacy, dignity, liberty, security, and presumption of innocence. Processing individuals' biometric data on such a massive scale cannot be reconciled with these rights.

Under the EU Charter of Fundamental Rights and the European Convention on Human Rights, any limitation of fundamental rights must be provided for in law, proportionate to the objective sought, and necessary to meet that objective. The deployments identified above largely serve to prevent petty crime and public disturbances, improve crowd control, and enhanced 'convenience'.

But their potential to serve these purposes is far outweighed by their interference with individuals' rights. This imbalance between the ends sought and the means used to achieve them points to the disproportionality of the deployments above.

In the 2013 case of Michael Schwarz v Stadt Bochum,[312] the CJEU ruled that if a data subject does not have a genuine chance to object to the collection of their personal data, their consent is undermined. Instances where a data subject is unable to object include most of the deployments above. These deployments do not inform individuals they are being surveilled, which makes it impossible for them to object to their data being collected.

The GDPR prohibits the processing of biometric data for the purpose of identifying individuals. There are several limited exceptions to this blanket ban of biometric data processing, and the Netherlands has added in some of their own. For example, the Netherlands' GDPR Implementation Act 2018 (AVG) allows for biometric data processing in cases where such processing is necessary for the purpose of security.

The example cited by a Dutch legislator regarding this exception is the hypothetical security of a nuclear power plant.[313] This sets the standard of an overriding interest justifying violation of the GDPR at a relatively high threshold.

In principle, the ends sought by private entities in their deployments are disproportionate reactions to the actions they wish to reduce. In terms of concrete legal opinions, a recent DPA/AP statement made it abundantly clear that crowd control and prevention of petty crimes cannot be considered serious enough overriding interests to constitute justification under the legislative guidance.

Beyond concerns of proportionality regarding deployments by private bodies, it is also useful to consider whether the measures are actually necessary and effective for their purpose. For example, in the trial of facial recognition surveillance technologies on public transport by RET, there were only 57 individuals with transport bans for the cameras to identify.[314]

Most deployments above follow this same pattern of deploying highly invasive systems for the purpose of identifying very low incidences of individuals. The trials can therefore be considered unnecessary and ineffective.

The extensive deployment of mass surveillance technologies to indiscriminately process individuals' personal biometric information, for the purpose of enforcing a ban against 57 people out of the roughly 620,000 populating the city, is an unnecessary reaction to what is clearly a relatively minor issue.

There are other measures that could be substituted for surveillance and biometric processing that would get the job done just as efficiently. The effectiveness of these trials is also questionable. There are cases of errors, for example with the F.C. Den Bosch facial recognition system detailed above. Artificial intelligence has worked demonstrably worse when processing the faces of women and minority ethnicities, raising issues of discrimination as well as being ineffective.[315]

311 **Paula Hooyman, 'Het ware gezicht van gezichtsherkenningstechnologie' Bits of Freedom (Amsterdam 2019), p. 21, available at:** https://www.bitsoffreedom.nl/wp-content/uploads/2019/11/het-ware-gezicht-van-gezichtsherkenningstechnologie.pdf

312 **(2013)** C-291/12.

313 **"The Dutch GDPR Implementation Act and the Use of Biometric Data" (2020)** https://www.akd.eu/insights/the-dutch-gdpr-implementation-act-and-the-use-of-biometric-data

314 **de Winter,** Nu.nl (2011).

315 **Lohr, S., 'Facial Recognition is Accurate, If You're a White Guy.' (New York Times, 2018) available at:** https://www2.cs.duke.edu/courses/spring20/compsci342/netid/readings/facialrecnytimes.pdf

# 3. LIVING LABS

## 3.1 Roermond

**Municipalities, the Dutch police, and some private entities collectively trial surveillance technology through so-called 'Living Labs', a term given to them by law enforcement authorities perhaps to emphasise their purported temporary existence.**

These labs tend to be concentrated in one city or neighbourhood. Citizens are often not informed of the project and its effect on their privacy and other fundamental rights. 'Living Labs' are theoretically only constituted for set periods of time, but in reality many remain operational after this time has expired.

In January 2019, the Dutch police launched a 'Sensing Project' at a shopping centre in the city of Roermond.[316] The Sensing Project is focused on what they have termed 'mobile banditry.'[317] This term is an inherently discriminatory version of shoplifting which by definition excludes Dutch nationals and focuses specifically on people that appear to be Eastern European.[318]

To determine if someone fits the presumed appearance, the police use criteria such as whether a person is travelling by car, whether they are accompanied by passengers, the specific route the car has taken to the shopping centre, and details of the car such as license plate, make, and model in order to profile them.[319]

These criteria are input into an algorithm which calculates a risk score - those with a high risk score generate a 'hit.'[320] The police are notified and tasked with responding. But patrol police have wide discretion and can decide which actions they will take. The most popular response is 'car interception.'

Under the Dutch Road Traffic Act 1994, the Dutch police can stop any car as long as they then check the driver's compliance with any road traffic rule laid down in the Act. By asking for license and registration, they check this box even if the true purpose of the stop was based on the predictive policing algorithm from the Sensing Project.

The collected data (i.e. ANPR (automated number plate recognition) data, model/colour of the vehicles, movement patterns) can be traced back to individuals via ANPR and so constitute personal data, therefore falling under the scope of the right to data protection. Data collected in the Sensing Project also qualifies as related to private life under Article 8(1) of the Charter of Fundamental Rights of the European Union.

Personal data processing in the context of policing and criminal law enforcement must be justified in part by its effectiveness in contributing to investigations. But when contacted by Amnesty International, the Dutch police were unable to demonstrate the effectiveness of the Sensing Project and admitted that the design of the project does not allow such a measure.[321]

The police also did not carry out a Data Protection Impact Assessment (DPIA) prior to processing the data, nor did police consult with the DPA/AP.

## 3.2 Eindhoven 'Living Lab'

Stratumseind 2.0 in Eindhoven is what is termed a 'Living Lab' where massive amounts of data (including biometric data) about people's activities is used to infer the effects of safety measures on crowd control and to study which factors contribute to violence and discomfort.

Officially, the public were notified that the lab intended to run from mid-2014 to mid-2018, but some of its projects seem to be continuing today (as seen on the Stratumseind 2.0 Facebook page).

The Stratumseind 2.0 project runs along Stratumseind street and includes five telephoto cameras, five sound meters, sensors, measuring instruments, and 22 LED lamp posts intended to influence the mood of the audience with the colour of their light.[322] All these devices collect real-time data, tracked in the information centre of the 'Living Lab'.

They measure visitor numbers, visitor origins and destinations, the effect of light, different sounds, weather, noise levels,

occupation of parking garages, crime statistics, amount of beer sold and trash collected, and much more. They also track social media, WiFi, modes of transportation used, messages on Twitter and Facebook, and analyse sentiment on social media.[323]

Data is received from these sources and from other sources including the police, beer brewers, Dutch Railways, KNMI, Road Safety and Transport Agency, and telecommunications providers (see image taken from a presentation by the City of Eindhoven in 2016).[324]

### 3.2.1 The CityPulse Project

Within the Stratumseind 2.0 'Living Lab', several other surveillance projects are also being carried out - most notably the CityPulse Project, the De-Escalate Project, and the Stratumse Poort project.

The CityPulse system was designed to analyse various types of data to search for anomalies in data patterns.[325] If these predictive systems predict that an incident is likely to occur, the regional police control room is notified.[326] The police would thus have the opportunity to make more informed decisions on potential actions to take on Stratumseind street.[327]

Cameras follow the movements of people within the crowd and interactions between them.[328] The people are visualised as dots on a floor plan of Stratumseind and these dots can be analysed to predict behaviour.[329]

For example, in the case of inferred aggression, movements and interactions between people will follow a certain pattern such as an accumulation of dots.[330] To verify these patterns, video is combined with sound analysis (details such as the volume of sound, its pitch, and inferred levels of anxiety within the voice).[331]

This analysis purportedly shows where aggression is taking place on the map.[332] The project developers claim that this is especially important if one of those dots is recognised by the system as a woman.[333]

---

316 **Amnesty International, 2020. We Sense Trouble. [online] London: Amnesty International Ltd. Available at:** https://www.amnesty.nl/content/uploads/2020/09/Report-Predictive-Policing-RM-7.0-FINAL-TEXT_CK-2.pdf?x53356

317 **Paula Hooyman, 'Het ware gezicht van gezichtsherkenningstechnologie' Bits of Freedom (Amsterdam 2019), p. 21, available at:** https://www.bitsoffreedom.nl/wp-content/uploads/2019/11/het-ware-gezicht-van-gezichtsherkenningstechnologie.pdf

318 **Ibid.**

319 **Ibid.**

320 **Ibid.**

321 **Ibid.**

322 **The Hague Security Delta, 'Stratumseind' Living Labs for Security Innovations (2020) available at:** https://www.thehaguesecuritydelta.com/innovation/living-labs/lab/3-stratumseind

323 **Merlijn Van Dijk, 'Stratumseind: Eindhoven's Data Street' Innovation Origins (2018) available at:** https://innovationorigins.com/stratumseind-eindhovens-data-street

324 **The Hague Security Delta,** Living Labs for Security Innovations (2020).

Additional video analysis software is being developed for recognising a clenched fist flying through the air.[334]

Video cameras of the CityPulse system had an embedded capability to track walking patterns.[335] The software can single out an individual with what it labels a 'suspicious walking pattern' on the street.[336]

Such a suspicious walking pattern could include someone walking up and down the street numerous times at a slow pace – apparently indicating the possibility of a theft.[337] Experiments with acoustic sensors raised the possibility of recognising the sound of fireworks or breaking glass and to determine their location very accurately.[338]

Dutch police officers have also been trialling body-cams in Stratumseind.[339] The most recent 'innovation' in technology in Stratumseind was in February 2020, when new motion sensors were tested during the carnival, measuring arm and leg movements. It was argued that carnival was the perfect opportunity to test the new sensors and to see if they still responded effectively if people were dressed up.[340]

In an interview with the Stratumseind 2.0 project leader, Tinus Kanters, he claimed that, at the time of writing (March 2018), when an incident of aggression is detected, the police are called and informed of where the incident is taking place through a GPS locator.[341]

The police then travel to the location, which takes around 30 seconds.[342] The project leader stated that, by the next summer (i.e. Summer 2018), an automatic signal would be sent to police in the case of detection of aggression, letting police know about an incident 'within seconds'.[343]

In the most recent article on the Stratumseind 'Living Lab' (February 2020), it seems that the system now notifies police who can then watch live on camera what is happening.[344]

---

325 **Security Management, 'Stratumseind Eindhoven: hoger veiligheidsgevoel én leuker door Living Lab' Achtergrond (2018) available at:** https://www.securitymanagement.nl/ stratumseind-eindhoven-living -lab/?vakmedianet- approve-cookies=1&_ga= 2.157495482.1453296129. 1606072868-157017026.1606072868

326 **Brainport Eindhoven, 'Kunstmatige intelligentie ondersteunt Stadstoezicht en politie tijdens carnaval' Nieuws (2020) available at:** https://brainporteindhoven.com/nl/nieuws/kunstmatige-intelligentie-ondersteunt-stadstoezicht-en-politietijdenscarnaval?tx_sitetemplate_newsletter%5Baction%5D=s ubscribe&tx_sitetemplate_newsletter%5Bcontroller%5D=Newsletter&cHash= 2f458f51cd681438376affe805a74e33

327 **Ibid.**

328 **Security Management,** *Achtergrond* (2018).

329 **Ibid.**

330 **Ibid.**

331 **Ibid.**

332 **Ibid.**

333 **The Hague Security Delta,** *Living Labs for Security Innovations* (2020).

334 **Ibid.**

335 **Merlijn Van Dijk, 'Stratumseind: Eindhoven's Data Street' Innovation Origins (2018) available at:** https://innovationorigins.com/stratumseind-eindhovens-data-street

### 3.2.2 The De-Escalate Project

The De-Escalate Project is a 'nudging tool' which tries to influence 'escalated behaviour.'[345] This project studied the use of 'interactive lighting design' in de-escalation by examining psychological pathways through which exposure to dynamic lighting might defuse escalating behaviour.[346] The experiment on the influence of light did not go well. Light did not appear to improve the atmosphere in the street and, in any case, this was very hard to measure.[347]

The De-Escalate Project also studied the effect of smell (i.e. oranges) on people's behaviour and found that citrus smells have a calming effect.[348] The way in which these effects are measured is highly invasive: the number of people on the street is measured, as well as their temperature and the number of fights inferred to be taking place.[349]

As body temperature can constitute a form of biometric data, in addition to other data that may be collected in pursuit of such experiments (such as gait or other crowd analytics), this amounts to biometric mass surveillance.

---

336 **Galic (2019),** Ars Aequi, p. 5.
337 **Ibid.**
338 **The Hague Security Delta, 'Stratumseind' Living Labs for Security Innovations (2020) available at:** https://www.thehaguesecuritydelta.com/innovation/living-labs/lab/3-stratumseind
339 **Wout van Arensbergen, 'Agenten filmen met bodycams lastige kroegbezoekers op Stratumseind in Eindhoven' ED (2017) available at:** https://www.ed.nl/eindhoven/agenten-filmen-met-bodycams-lastige-kroegbezoekers-op-stratumseind-in-eindhoven~a3ba64c8
340 **Brainport Eindhoven, 'Kunstmatige intelligentie ondersteunt Stadstoezicht en politie tijdens carnaval' Link Magazine (2020) available at:** https://www.linkmagazine.nl/kunstmatige-intelligentie-ondersteunt-stadstoezicht-en-politie-tijdens-carnaval
341 **Security Management,** Achtergrond (2018).
342 **Ibid.**
343 **Security Management, 'Stratumseind Eindhoven: hoger veiligheidsgevoel én leuker door Living Lab' Achtergrond (2018) available at:** https://www.securitymanagement.nl/ stratumseind-eindhoven-living-lab/?vakmedianet- approve-cookies=1&_ga= 2.157495482.1453296129. 1606072868-157017026.1606072868
344 **Brainport Eindhoven, 'Kunstmatige intelligentie ondersteunt Stadstoezicht en politie tijdens carnaval' Link Magazine (2020) available at:** https://www.linkmagazine.nl/kunstmatige-intelligentie-ondersteunt-stadstoezicht-en-politie-tijdens-carnaval
345 **Diede Hoekstra, 'Netwerk van hypermoderne camera's op Stratumseind in Eindhoven gaat politie helpen' ED (2017) available at:** https://www.ed.nl/eindhoven/ netwerk-van-hypermoderne-camera-s-op-stratumseind-in-eindhoven-gaat-politie-helpen~a1e8acee

### 3.2.3 The European Project

Experiments at Stratumseind also focused on attempted community-building between citizens and law enforcement, seeking to allow citizens to notify police of incidents via their phone and vice versa.[350] The 'European project' this is associated with (no further information given) aims to translate video into text. This utilises a wealth of video data, which is time-consuming to manually analyse. For example, if one searches 'man with dog', the system will be able to pinpoint relevant video stills.[351]

Another similar experiment concerns the identification of reckless driving or drivers 'showing off', such as when a driver noisily drives through the street a number of times. The 'Living Lab' aims to examine whether it is possible to identify the car or driver and accordingly issue a visual or auditory warning.[352] More information is needed but given the intrusiveness of other such 'Living Lab' experiments it is likely that biometric mass surveillance may be a feature where the identification of such drivers is concerned.

## 3.3 Utrecht

The 'Living Lab' in Utrecht consists of burglary predictors, a social media monitoring room, smart bins, and smart streetlights with sensors of which the city does not provide warnings.[353]

There are also scanner cars that dispense parking tickets, but also detect residents with municipal tax debt.[354] There is a programme labelled by one city official as 'targeted and innovative supervision' which keeps track, through mobile devices, of the number of young people hanging out on the street, their age group, whether they know each other or not, the atmosphere, and whether or not they 'cause a nuisance.'[355]

Council documents justify these programmes by citing their help in predictions of school drop-outs, predictions of poverty, and the monitoring of "the health of certain groups" with the aim of "intervening faster." The city argues it is not violating privacy laws because they anonymised/pseudonymised the data.

A journalist from the Guardian investigating the Utrecht 'Living Lab' was referred by the city to a private company for many questions.[356] This company was not identified by the article. This highlights the trend of public authorities outsourcing tasks to private companies (waste removal, street lighting, etc) without making agreements about ownership of the data collected.

An example is CityTec, a company that manages 2,000 car parks, 30,000 traffic lights, and 500,000 lamp posts in the Netherlands.[357] The company refuses to share with municipalities the data it was collecting through sensors on lamp-posts throughout the infrastructure it owned and operated. It is unclear what the company is doing with this data.[358]

346 Ibid.
347 Ibid.
348 Ibid.
349 Ibid.
350 Ibid.
351 Ibid.
352 The Hague Security Delta, Living Labs for Security Innovations (2020) available at: https://www.thehaguesecuritydelta.com/innovation/living-labs/lab/3-stratumseind
353 Guardian staff reporter. "'Living Laboratories': The Dutch Cities Amassing Data on Oblivious Residents." (The Guardian 2018) www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht
354 Ibid.
355 Ibid.
356 Ibid.
357 Ibid.
358 Ibid.

## 3.4 Enschede

In Enschede, city traffic sensors pick up your phone's WiFi signal even if you are not connected to a WiFi network.[359] Trackers can register your MAC address, which is the unique network card number contained in every smartphone.[360]

The municipality says it is saving €36m in infrastructure investments by launching a smart traffic app that rewards people for good behavior like cycling, walking, and using public transport.[361] But the fine print of the app says it creates "personal mobility profiles" and that the collected data belongs to the private company Mobidot.[362]

## 3.5 Legal Analysis

Fundamental rights such as those in the ECHR and EUChFR are difficult to reconcile with 'Living Labs'. These programmes treat entire neighbourhoods and cities as experimental subjects, often without informing individuals living in these areas.

Article 1 of the Charter contains strong language regarding the right to human dignity. Numerous other human rights - such as that to privacy – share the right to dignity as a key foundation.[363]

By collecting and processing deeply personal, individualised data from all residents and visitors to a city or neighbourhood, 'Living Labs' can be said to violate human dignity on a massive scale. The EUChFR proclaims human dignity to be 'inviolable.'[364]

This implies that, even if biometric surveillance technologies were justified as a security imperative, the member state would still have to ensure dignity is not being violated.

In the case of 'Living Labs', the violation of human dignity is compounded by the disproportionality of the ends sought with the means used. All of these 'Living Labs' have the same object as private deployments, but on a much larger scale.

They purport to stop petty crimes and public disturbances, such as shoplifting and fighting. But reducing - or even eliminating - these crimes is not enough of an overriding interest to justify such large-scale, indiscriminate collection of individuals' intimate biometric information.

Not only do these 'Living Labs' violate the human dignity of individuals on a massive scale, but they do so for a purpose that is vastly less important and less urgent than Dutch legislators intended. The example provided which would justify using facial recognition surveillance technology for security purposes was in the case of a nuclear power plant.[365]

The reduction of petty crime and public disturbances is plainly not on the same level as this example.

Because of these significant concerns, in 2019 the Dutch DPA started an investigation into these 'smart cities.' Even though this investigation has not yet been concluded, the head of the DPA/AP unequivocally stated that digitally following people in semi-public (aka privately-owned but publicly-accessible) spaces is a breach of privacy which is only permitted in

specific circumstances, requiring at least a sufficiently clear and precise legal basis and predictability in the application of these technologies.[366]

Furthermore, privacy risks must be addressed and managed in advance of the project starting.[367] Considering the concerns mentioned above, it is unlikely that the 'Living Labs' in this section comply with these requirements, further reinforcing the fact that they are a grave breach of human rights and privacy rights.

As 'Living Labs' tend to involve the police, it is necessary to look at national laws regarding law enforcement and data processing. According to the WPG, police data (defined as any instance where personal data is processed for the purpose of policing duties) may be collected in the context of regular policing duties (i.e. enforcing laws and directing traffic).[368]

However, the data subject must be informed that their information is being processed.[369] In cases of mass surveillance such as 'Living Labs', it is often impossible for individuals to be aware that their data is being collected.

The location of surveillance cameras is not always obvious, and systems that track your online footprint such as the WiFi sensors in Enschede are virtually undetectable.

It is therefore reasonable to conclude that most individuals visiting areas where 'Living Labs' are in operation will be unaware of the surveillance they are being subjected to by merely existing in that specific location.

A common theme with 'Living Labs' is that their temporal limitation purportedly gives them some kind of extralegal jurisdiction, allowing them to freely contravene the law.[370] But in many cases, the surveillance technologies are deployed long after the project was intended to expire.

And, regardless of the truth behind these 'Living Labs' being temporary, it is simply not true that temporal restrictions on a violation of human rights, EU law, and national law neutralises those violations.

---

359 **Ibid.**
360 **Ibid.**
361 **Ibid.**
362 **Ibid.**
363 **Barak, A., Human Dignity: The Constitutional Value and the Constitutional Right (2016) Human Rights Law Review, 16(1), 156-169** https://doi.org/10.1093/hrlr/ngv042
364 **EChFR,** Article 1.
365 **Supra n.** (102).
366 **Autoriteit Persoonsgegevens, 'Waarborg privacy in de ontwikkeling van Smart Cities' Nieuws (2019) available at:** https://autoriteitpersoonsgegevens.nl/nl/nieuws/waarborg-privacy-de-ontwikkeling-van-smart-cities
367 **Ibid.**
368 **Supra n.** (27).
369 **Ibid.**
370 **Ibid.**

# 4. CONCLUSION

**This section focusing on the Netherlands has shown that the use of biometric mass surveillance technologies, in particular facial recognition surveillance technologies, is widespread and increasing in the Netherlands and adversely impacts a worryingly large number of people, often without their knowledge.**

Biometric surveillance technologies are used by actors in both the public and private sectors, for a variety of purposes and by entities large and small. More often than not, such deployments of biometric surveillance technologies have a questionable legal basis, or no legal basis at all, and they often blatantly breach data protection laws or infringe upon fundamental human rights such as privacy in a manner that cannot be justified as proportionate, legitimate, reasonable, or necessary.

Furthermore, a lack of transparency makes it difficult for citizens and advocates alike to keep up with rapid developments in this area, to hold actors using biometric surveillance technologies to account, and to initiate a public debate on these issues. Particularly worrying are increasing applications by Dutch police of facial recognition technology to the criminal justice database of CATCH, exacerbated by the fact that the police are failing to remove the data of those who have been found innocent.[371]

Another concerning development is the fact that the illegal collection and processing of biometric data by private actors goes largely unpunished, as the Dutch DPA/AP does not have the capacity to enforce privacy laws on a large scale.

A final unsettling finding which emerged in this report is the widespread use of the somewhat sinisterly named 'Living Labs', which take citizens' biometric data and turn it into an experiment, contrary to their knowledge or consent, egregiously interfering with their basic human dignity and fundamental, universally-recognised human rights as protection by domestic law, regional law, and international law.

Given the scale of biometric surveillance in the Netherlands, a democratic conversation about these issues is urgently necessary. In November 2019, a motion was passed in the Second Chamber of the Dutch Parliament which called on the government to examine the legal framework applicable to facial recognition technology and to revise and update it.[372]

A revision of the applicable legal framework creates an opportunity for the Netherlands to strengthen and entrench legal protections which address the violations of human and privacy rights commonly associated with biometrics.

The law is currently out of pace with technology, but it is not yet too late to address this, as demonstrated by San Francisco, which banned facial recognition technology in 2019.[373] In a similar vein, a motion was recently passed in the Dutch Second Chamber of Parliament to improve the capacity and resources of the Dutch DPA/AP, which could address the structural enforcement problem discussed throughout this country-specific section.[374] While these motions are steps in the right direction, signs to the contrary are also emerging.

For instance, renewing the Wbvk as discussed in section 1.1.2.1 against the advice of the DPA/AP would pose a barrier to these potential improvements to the landscape of biometrics in the Netherlands, considering the widely recognised

371 **Hulsen,** *Nu.nl* (2021).

372 **Tweede Kamer der Staten-Generaal, Motie van de leden Verhoeven en Van Dam over het wettelijk kader voor gezichtsherkenningstechnologie (Motion 35300-VI-64, 21st of November 2019) available at:** https://www.tweedekamer.nl/kamerstukken/detail?id=2019Z22945&did=2019D47541

373 **Veena Dubal, 'San Francisco was right to ban facial recognition. Surveillance is a real danger' The Guardian (2019) available at:** https://www.theguardian.com/commentisfree/2019/may/30/san-francisco-ban-facial-recognition-surveillance

374 **Tweede Kamer der Staten-Generaal, Motie van het lid Van Beukering-Huijbregts c.s. over de capaciteit bij de Autoriteit Persoonsgegevens (Motion 35570-VI-62, 26th of November 2020) available at:** https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2020Z22977&did=2020D48569

375 **Supra** (n 70).

376 **For the text of the law as it currently stands, see:** Eerste Kamer der Staten-Generaal, Wet gegevensverwerking door samenwerkingsverbanden

377 **Platform bescherming burgerrechten, 'SyRI-coalitie aan Eerste Kamer: 'Super SyRI' blauwdruk voor meer toeslagenaffaires' Nieuws (11 January 2021) available at:** https://platformburgerrechten.nl/2021/01/11/syri-coalitie-aan-eerste-kamer-super-syri-blauwdruk-voor-meer-toeslagenaffaires; Amnesty International, 'Kabinet, voorkom toeslagenaffaire in het kwadraat' Nieuws (18 January 2021) available at: https://www.amnesty.nl/actueel/kabinet-voorkom-toeslagenaffaire-in-het-kwadraat

378 **Peter te Lintel Hekkert, 'Eerste Kamer trapt op de rem bij Super SyRI' FNV (19 January 2021) available at:** https://www.fnv.nl/nieuwsbericht/sectornieuws/uitkeringsgerechtigden/2021/01/eerste-kamer-trapt-op-de-rem-bij-super-syri

violations of privacy rights it creates.[375] Another law currently going through the Dutch Parliament is the so-called 'Super SYRi' law, or the 'Wet Gegevensverwerking door samenwerkingsverbanden'.[376]

This law would authorise the far-reaching exchange of personal data between different government departments and between government departments and private companies, and has been heavily criticised for its lack of human rights guarantees by civil society organisations.[377]

While the First Chamber of Parliament has currently paused the passage of this law, developments in this area should be closely monitored by digital rights advocates, considering the scale of biometric data held by Dutch public bodies. [378]

# INTRODUCTION TO POLAND COUNTRY STUDY FROM EDRI:

**Whilst biometric mass surveillance practices (such as the remote biometric identification of individuals in public spaces) are less prevalent in Poland than in the Netherlands and Germany, Poland is far from being a biometric mass surveillance-free society – and is likely to follow the Netherlands' and Germany's leads in translating databases and infrastructure into widespread biometric mass surveillance.**

Although Poland's Constitution enshrines people's rights to dignity and informational autonomy, as well as European rights to privacy, data protection, and non-discrimination (among others), practices which are creating the perfect conditions for biometric mass surveillance are on the rise.

Given Poland's self-styled desire to be a leading country for artificial intelligence (AI) and digital governance, it is particularly worrying that these technological developments occur against a backdrop of democratic backsliding, threats to the rule of law, and the suppression of freedoms of association and expression, in particular for women and LGBT+ groups.

The first example in this Poland report, which analyses the 2020 Home Quarantine app which was implemented to enforce quarantine at the start of the COVID-19 pandemic, suggests that Poland is a state not properly equipped (legislatively or practically) to deal with the fundamental rights challenges posed by the growing impulse to identify and track people via their biometric data.

Poland's swift move to use facial recognition as a way to monitor and track the population's adherence to quarantine measures was neither necessary nor proportionate for the aim sought, with cost and efficiency placed before people's fundamental rights.

This mandatory app also saw a lucrative public-private partnership stood up in just three days, focused around the use of facial recognition.

Particularly worrying was the fact that the retention periods for said biometric data put the burden of deletion on the user. Coupled with evidence of abusive use of the app by police against individuals that were longer in quarantine, and the fact that the initially voluntary app was suddenly made mandatory without justification, this example reveals an ideology of pushing facial recognition into products and services without good reasons to do so.

Second, the research analyses the case of the introduction of mandatory biometric data in national Polish identification cards. This reveals a desire to gather more and more of citizens' and residents' biometric data without proper justification for such an expansion.

Individuals in Poland as young as 12 are mandated to submit their biometric data in order to receive a compulsory ID, and the research reveals a grave mismatch between the purported European 'benefit' of the IDs for free movement and national security compared to the ways in which they are used in reality, which is largely for national civic purposes, thus challenging the necessity of the collection of biometric data.

Beyond these issues, the expansion of Polish national IDs to include biometric data includes statutory loopholes for sharing the data with a wide range of government agencies and worrying provisions for the indefinite retention of face biometrics.

The third example reveals how, whilst the security service surveillance operations of EU member states remain in the jurisdiction of said state, the example of Poland can provide us with an important glimpse into the ways in which intelligence schemes can still pose a threat of biometric mass surveillance against part or whole populations.

The secretive procurement of a 5 million euro "Pegasus" spyware system with biometric data collection capabilities has been deployed widely in Poland, despite a total lack of oversight and the association of this particular system with the killing of journalists and the suppression of human rights defenders in third countries.

It provides a cautionary tale about how targeted surveillance can, in many ways, be just as harmful and discriminatory as "indiscriminate" biometric surveillance; and how its secretive and un-regulated use – without judicial safeguards or any oversight body – can still create a perception of mass surveillance across the population.

Across the Polish examples, we see a series of actions that may be leading to the normalisation of the collection of biometric data collection and processing – contrary to EU rules – and which also create databases and infrastructures that are ripe for biometric mass surveillance.

The time is nigh for authorities to curtail these databases and practices, and proactively put in place rules that will make sure that biometric mass surveillance practices are well and truly banned.

This is why EU Member States and EU institutions need to step up and ban biometric mass surveillance practices in order to safeguard people's fundamental rights. Such a ban requires that abusive and unlawful deployments remain the absolute exception – never the norm.

# POLAND

**Prior to the implementation of the General Data Protection Regulation (GDPR), Polish law did not recognise biometric data as a unique form of personal data. Consequently, the implementation of the GDPR constitutes an important step in the consolidation of privacy rights in Poland - a country that within living memory endured the political winter of the former Eastern Bloc. The country's past has created a legacy of historically-rooted discomfort towards state surveillance regimes and the suggestion of implementing such regimes for any reason.**

In comparison to many Western European jurisdictions, the prevalence of biometric mass surveillance in Poland appears to remain low. However, this report has found that the implementation and risks of biometric surveillance technologies in Poland appear to be rising in a domestic context where the scrutiny of surveillance practices is seemingly lacking.

In comparison to many Western European jurisdictions, the prevalence of biometric mass surveillance in Poland appears to remain low. However, this report has found that the implementation and risks of biometric surveillance technologies in Poland appear to be rising in a domestic context where the scrutiny of surveillance practices is seemingly lacking.

This section focuses on 3 key deployments of biometric processing technologies and/or biometric surveillance technologies in Poland: namely **(1)** the creation of a compulsory home quarantine app in response to the current COVID-19 pandemic; **(2)** a biometric ID bill recently passed by the Polish Parliament ("Sejm") for the purpose of improving cross-border security; and **(3)** the suspected purchase and use of a spyware programme known as Pegasus by Poland's Central anti-Corruption Bureau.

Before these three deployments are presented and analysed, this report shall set out the domestic legal framework governing the processing of biometric data and the ways in which surveillance apparatus may be used more generally.

This is because Poland, in contrast to Germany and the Netherlands, lacks a coherent or comprehensive set of legal acts governing this area of the law. This incomplete and outdated framework, in turn, may serve as an enabling tool for public authorities to engage in surveillance practices, including biometric mass surveillance.

# 1.THE DOMESTIC LEGAL FRAMEWORK

## 1.1 An Overview

Poland's domestic legislation governing the use of personal data, including biometric surveillance, is fragmented. There is no single domestic Act, regulation, or other legal instrument that governs when such data can be gathered, processed, or stored. As such, Polish law relies heavily on the GDPR as an institutional safeguard against the illegal, unnecessary, or disproportionate collection and use of such data.

However, a wide variety of state organs in Poland are authorised to collect personal data (including biometric data), principally for administrative or surveillance purposes.[379] These authorities are thus governed domestically at the highest level by the Polish Constitution, but also by a patchwork of legislative acts.

[379] **See Act of 9th June 2006** on the Central Anti-Corruption Bureau Arts. 17-18; Act of 24th May 2002 on the Internal Security Agency and Foreign Intelligence Agency Arts 27-28; Act of 9th June 2006 on the Military Counter-Intelligence Service and Military Intelligence Service Arts. 31-32; the Act of 12th October 1990 on the Border Guard Arts. 9e and 10b.

## 1.2 The Constitution

Poland's relationship with surveillance post-1989 is one marked by profound public distrust of the State - a result of the country's Communist past, which saw State surveillance organs used to suppress political dissent.[380] The current Polish Constitution echoes this broader sentiment by setting out a series of principles that - in their practical application - should limit the mandate possessed by the country's various surveillance agencies.

At the broadest level, Article 2 stipulates that the Polish state shall be democratic and ruled by law. Article 7 elaborates on this principle, stipulating that the country's public authorities shall operate through and within the limits of the law - including, by extension, those public authorities with the power to launch surveillance operations.

Against this backdrop, Chapter II of the Constitution sets out a Bill of Rights of sorts, describing the positive rights enjoyed by Poland's citizens.

This includes three rights directly relevant for the purposes of surveillance: Article 47 enshrines the right to the protection of one's private and family life; Article 49 sets out the right to freedom and secrecy of personal communication; while Article 51 sets out the right to informational autonomy.

These provisions can be read in conjunction with Article 30, which ties these rights under the protection of human dignity and reaffirms that such rights must enjoy respect and protection from all public authorities.

Finally, Article 31(3) stipulates that any restriction on a citizen's personal rights must result from statute and only when necessary in a democratic state for, *inter alia*, the protection of state security and public order.

380 **Jan Podkwik, "Privacy in the Digital Era - Polish Electronic Surveillance Law Declared Partially Unconstitutional", European Constitutional Law Review,** Vol 11 Issue 3 pg. 577, 588.

381 **Ustawa z 10 maja 2018 o ochronie danych osobowych** [Protection of Personal Data Act] (Dz. U. 2018, item 1000).

382 **Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania** [Amendment Act] (Dz. U. 2019, item 730).

383 **Decyzja Prezes Urzadu Ochrony Danych Osobowych z dnia 18 lutego 2020 r, available at** https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018

384 **'Dane biometryczne moga być wykorzystywane tylko w wyjatkowych sytuacjach' (UODO, 3rd March 2021)** https://uodo.gov.pl/pl/138/1943

## 1.3 The GDPR

The GDPR has applied in Poland since its entry into force on 25 May 2018. While directly applicable, two key Acts were passed by the Sejm to facilitate its implementation: the Act of 10 May 2018 on the Protection of Personal Data;[381] and the Act of 21st Feb 2019 on the amendment of certain acts in connection with ensuring the application of the GDPR.[382] Each Act shall be addressed in turn.

### 1.3.1 The Act of 10th May 2018

The Act of 10th May 2018 created a new supervisory authority in Poland on the gathering and use of personal data, including biometric data - the Office of Personal Data Protection ("urząd ochrony danych osobowych" or "UODO").

This new body replaced Poland's previous personal data protection authority – the General Inspector of Personal Data Protection ("generalny inspektor ochrony danych osobowych" or "GIODO"). The UODO organisation represents Poland on the European Data Protection Board.

Since its inception, the UODO has only dealt with one case concerning the use of biometric data specifically.[383] However, on March 3rd, 2021, the UODO published guidance concerning the collection and processing of biometric data by private and public entities in Poland.[384]

### 1.3.2 The Act of 21st February 2019

The Act of 21st February 2019 sought to amend Poland's existing laws to ensure compliance with the GDPR. The law's scope was broad, amending 162 pre-existing domestic Acts in total.

## 1.4 The Office of Personal Data Protection ("UODO")

As noted above, the Office of Personal Data Protection ("UODO") was created by Chapter 6 of the Act of 10th May 2018 to replace the General Inspector of Personal Data Protection, in order to ensure domestic compliance with the GDPR.

The UODO - and its pre-GDPR predecessor the GIODO - have both encountered cases concerning biometric data. The GIODO dealt with a string of cases concerning the use of biometric fingerprint scanners by public and private employers for security services.[385]

However, since the implementation of the GDPR, the new UODO has only issued one fine for the breach of biometric, as opposed to other forms of personal, data – in which a Gdańsk primary school was fined for scanning the fingerprints of children as a means to verify whether the child had paid for a school meal.[386]

385 **See Decision of 22 February 2008 (DIS/DEC-134/2405/08), Writing of 15 December 2009** (DIS / DEC-1261/46988/09), Judgement of the Supreme Administrative Court of 1st December 2009 (I OSK 249/09).

386 **President of the UODO, Decision (ZSZZS.440.768.2018), available at** https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018

In this case, the Personal Data Protection Officer of the UODO emphasised that the processing of biometric data is allowed only in exceptional situations listed in the GDPR and under strictly prescribed conditions. He deemed a failure to abide by such conditions "*may pose a serious risk to fundamental rights and freedoms*", before finding the "uniqueness and permanence of biometric data" necessitates "particular caution and diligence".[387]

He emphasised this was especially so where children are concerned, since any uncontrolled leakage "will not be reversible in time, even after the child reaches the age of majority."[388]

While both the UODO and former GIODO have encountered and dealt with the use of biometric data, such encounters seem to have occurred in the context of private employers or by public administrative entities, and not for law enforcement purposes.

Neither appear to have yet dealt with cases of the deployment or potential deployment of remote public biometric identification systems in Poland. However, this is not conclusive proof that such deployments have not occurred, but rather that the data protection authorities have not yet dealt with any such deployments.

Thus, while both the UODO and its predecessor – the GIODO – have dealt with instances involving the use of biometric data, such encounters have occurred in seemingly discreet, small-scale instances.

However, this state of affairs doesn't necessarily point to an absence of general mass deployments. Often, smaller incremental biometric deployments offer a backdoor means for states to create a mass surveillance infrastructure over time.

Furthermore, it must be noted that even if the UODO has not investigated instances of biometric mass surveillance deployments to date, this does not mean that such deployments are not occurring on the ground. Indeed, the UODO has failed to investigate any of the three key biometric deployments set out in the following sections of this report at the time of writing.

This points to a potential failure of the part of the UODO to properly scrutinise the potential deployment of biometric mass surveillance in Poland.

387 Ibid.
388 Ibid.

## 1.5 Other Acts Governing Surveillance

In Poland, with the exception of the GDPR and its two implementing Acts, there is no bespoke legislation regulating biometric surveillance specifically. Similarly, there is no centralised Act that governs the use of surveillance generally. Instead, the law has allowed for the creation of a patchwork of intelligence agencies (known in Poland as "special services"[389]) with the power to conduct surveillance operations.[390]

Key among these are the Central Anti-Corruption Bureau,[391] Internal Security Agency,[392] Border Guard,[393] the Military Counter-Intelligence Service, and the Military Police.[394] These organisations are permitted to conduct surveillance operations, respectively, under the:

**1.** Act of 9th June 2006 on the Central Anti-Corruption Bureau ("Ustawa o Centralnym Biurze Antykorupcyjnym"), Arts. 17-18;
**2.** the Act of 24th May 2002 on the Internal Security Agency and Foreign Intelligence Agency ("Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu"), Arts 27-28;
**3.** the Act of 9th June 2006 on the Military Counter-Intelligence Service and Military Intelligence Service ("Ustawa o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego") Arts. 31-32; and
**4.** the Act of 12th October 1990 on the Border Guard ("Ustawa o Straży Granicznej"), Arts. 9e and 10b.

It must be noted that these provisions deal primarily with the interception of communications (i.e., wiretapping) and the collection of metadata (e.g., location data). As such, they regulate 'traditional' means of surveillance but do not appear to foresee the cutting-edge biometric technologies which form the focus of this report. This is likely a product of the drafters not envisaging the emergence of new biometric technologies at the time of drafting.

389 **Mateusz Kolaszyński,** 'Overseeing surveillance powers - the cases of Poland and Slovakia' pg. 3.
390 **Ibid.**
391 **"Centralne Biuro Antykorupcyjne" or "CBA".**
392 **"Agencja Bezpieczeństwa Wewnetrzego" or "ABW".**
393 **"Straż Graniczna".**
394 **"Służba Kontrwywiadu Wojskowego".**

# 2. "KWARANTANNA DOMOWA" – POLAND'S HOME QUARANTINE APP

## 2.1 An Overview

On March 19 2020, Poland became one of the first countries in the world to create an app to monitor self-isolation compliance in the COVID-19 pandemic.[395] The app – known as Kwarantanna Domowa or "Home Quarantine" – was initially introduced by the Ministry of Digitalisation as an optional tool for those required to self-isolate.[396]

However, from 1 April 2020, the app became mandatory.[397] As a consequence, downloading the app is now a legal requirement for all individuals required to self-isolate in Poland, subject to a limited list of exemptions.[398] Falsely claiming to fall under one these exemptions is a criminal offence,[399] which can lead liability under Art. 233(1) of the Criminal Code.[400]

The app was allegedly developed with the aim of improving the efficiency and cost of monitoring COVID-19 self-isolation compliance, by reducing the amount of police time and expenditure spent on home visits.[401]

The app tracks users through a combination of geolocation and facial recognition,[402] which seek to verify the user's location and identity, respectively.[403] As such, the app allows the authorities to monitor individual compliance with self-isolation requirements remotely.[404]

Citizens required to self-isolate first receive an SMS message requiring them to download the 'Home Quarantine' app.[405] On completion of this, users are then required to perform an initial task known as "quarantine full information", whereby they must submit a "selfie" photo at their declared place of quarantine.[406]

This photo becomes a reference photo which is compared with each subsequent photo taken in the course of the user's isolation period.[407] Having executed this initial task, app users are then required to take and submit selfies when randomly notified by the app.[408] Upon being notified, users are given twenty minutes to take and send a facial image.[409]

The app then uses facial recognition technology to confirm the identity of the phone-user and GPS to determine their location.[410] A failure to perform these tasks within the allotted time frame leads the app to automatically send a notification to the police.[411]

The Home Quarantine app was developed by the Ministry of Digital Affairs in partnership with the Ministry of Health and TakeTask, a Warsaw-based company that creates software for enterprises and institutions.[412]

The company, which earned PLN 2.5 million on commission for developing the app, claims the Minister of Digitalisation chose them for, among other reasons, the high care of data security provided by their software.[413] The app is said to operate via an independent Microsoft Azure server, owned by the Ministry of Digital Affairs.[414]

Following the app's initial launch in March 2020, the Ministry of Digitalisation concluded a new, 12-month contract with the company TakeTask on June 19 2020.[415]

The app's privacy and security provisions are found in section 9 of the Regulations of the "Home Quarantine App".[416]

According to this provision, the Minister of Digital Affairs is the administrator of the personal data collected,[417] and can process, among other features, a citizen's

395 **Mark Scott and Zosia Wanat, 'Poland's coronavirus app offers playbook for other governments' (Politico, 2 April 2020)** https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments

396 **Katri Uibu, 'Poland is making its citizens use a 'selfie' app during the coronavirus crisis' (ABC, 24 April 2020)** https://www.abc.net.au/news/2020-04-25/coronavirus-poland-tracking-quarantine-selfie-app/12173884

397 **via the insertion of Art. 7e of Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiazaniach zwiazanych z zapobieganiem,** przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych [Act of March 2 2020 on Special Solutions Relating to the Prevention, Counteracting and Combating of Covid-19, other Infectious Diseases and Emergencies Caused by them] (Dz. U. 2020, item 374).

398 **Ibid.** Art 7e(2).

399 **Ibid.** Art 7e(3).

400 **"Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny" [Criminal Code] (Dz. U. 1997, item 553)** http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970880553

401 **Panoptykon Foundation, 'Odpowiadamy na pytania o aplikacje „Kwarantanna domowa" (25 March 2020)** https://panoptykon.org/aplikacja-kwarantanna-domowa

402 **Polish Goverment, 'Aplikacja „Kwarantanna domowa" – to musisz wiedzieć' (10 April 2020)** https://www.gov.pl/web/cyfryzacja/aplikacja-kwarantanna-domowa--to-musisz-wiedziec

403 **See supra** (n23).

404 **Ibid.**

405 **See supra** (n19) Art. 7e(1).

406 **para. 6(1) Regulamin aplikacji "Kwarantanna domowa" [Regulations and Privacy Policy], available at** https://www.gov.pl/web/koronawirus/kwarantanna-domowa-regulamin

407 **Polish Government, 'Aplikacja Kwarantanna domowa – od dziś-obowiazkowa' (1 April 2020)** https://www.gov.pl/web/koronawirus/aplikacja-kwarantanna-domowa--od-dzis-obowiazkowa

408 **para. 6(3)** Regulations.

409 **para. 6(4)** Regulations.

410 **See supra** (n29).

411 **para. 6(7)** Regulations.

facial image and location[418] (including the declared address for quarantine and the location designated by the system during the verification task).

The authorities that have access to a citizen's picture and location, among other data, are listed under section 9(3) as: the Police Headquarters; the Provincial Police Headquarters; the Voivodes (provinces); the Central Information Technology Centre; TakeTask SA; and the Centre for Healthcare Information Systems.

As per section 9(11), the Minister of Digital Affairs stores the ordinary personal data collected by the app for the period specified in art. 118 of the Civil Code – namely, 6 years. However, the Regulations make an exception for facial images, which are instead deleted when the account is deactivated.[419]

412 **Wprost, 'Za aplikacje „Kwarantanna domowa" odpowiada polska spółka TakeTask. Inne kraje też zainteresowane' (7 April 2020)** https://biznes.wprost.pl/technologie/10313034/za-aplikacje-kwarantanna-domowa-odpowiada-polska-spolka-taketask-inne-kraje-tez-zainteresowane.html

413 **Ibid.**

414 **Ibid.**

415 **Money, '"Kwarantanna domowa" bedzie działała rok dłużej. Resort cyfryzacji przedłużył umowę z twórcami aplikacji' (4th July 2020)** https://www.money.pl/gospodarka/kwarantanna-domowa-bedzie-dzialala-rok-dluzej-resort-cyfryzacji-przedluzyl-umowe-z-tworcami-aplikacji-6528240382727809a.html

416 **para. 9** Regulations.

417 **para. 9(1)** Regulations.

418 **para. 9(3)** Regulations.

419 **para. 9(11)** Regulations.

## 2.2 Analysis

### 2.2.1 Legal Basis

The legal basis for a compulsory Home Quarantine app is found via the insertion of Art. 7(e) in the "Act of March 2, 2020 on special solutions relating to the prevention, counteracting and combating of COVID-19, other infectious diseases and emergencies caused by them".[420] Thus, there appears to be a domestic legal basis for the collection and processing of facial images.

It is worth noting that the processing of photographs alone does not automatically constitute biometric data under the GDPR.[421] However, as per Recital 51 GDPR, photographs will be treated as a special category of data under Article 9 to the extent they allow the unique identification or authentication of an individual.

Given the purpose of the "selfie" requirement on the Home Quarantine App is to verify the identity of the user, the use of facial images in this context seem to clearly constitute biometric data for the purposes of Article 9.

Thus, it is next necessary to determine whether the App is compliant with the rules that apply to the "sensitive data" listed in this Article. As per Article 9(1) of the GDPR, the collection of biometric data is prohibited unless subject to an exception listed under Article 9(2). Included in Article 9(2) is the lawful collection of biometric data for reasons of public interest where necessary in the area of public health.

Given the Home Quarantine App possesses a legal basis in Poland's domestic law, and there is a public interest in enforcing self-isolation requirements, the App appears at face value to be compliant with Article 9 GDPR.

However, concerns have been raised by NGOs including the Panoptykon Foundation as to the necessity and proportionality of biometric data processed on the App, as well as the transparency of the process under which it became a legal requirement for individuals within Poland.[422]

It is worth noting that the exception under Article 9(2) requires any measure to be necessary in the area of public health. Consequently, the legal analysis on this report shall focus primarily on the necessity of the Home Quarantine App. It shall then turn to the wider implications the Home Quarantine app may have on the likelihood of biometric surveillance being conducted in the future.

### 2.2.2 Necessity and Proportionality

Poland is not the first or only country to have introduced measures on citizens' phones in response to the COVID-19 pandemic. In Singapore, a smartphone app has used Bluetooth to trace whether individuals have come into contact with infected persons,[423] while Taiwan has introduced "electronic fences" to alert the authorities where self-isolating citizens leave their homes.[424]

However, Poland's Home Quarantine app is seemingly unprecedented in obliging users to submit images of their faces for the purpose of biometric processing.

The government's act of resorting to such an extreme measure, in light both of the alternatives available and the context in which the app came into existence, raises fundamental questions concerning the premise of whether facial recognition is necessary or proportionate for the objective of protecting public health.

This is especially pertinent in light of the particular sensitivity of biometric data and the unique protections such data enjoys under the GDPR.

Prior to the app's creation, Poland monitored the compliance of those self-isolating through regular unannounced home visits by the police.[425] This approach was in line with that of most EU Member States, who tended either to take a

deferential approach to self-isolation requirements or else would enforce compliance through the use of civil penalties.[426]

On March 19, 2020, the police noted only 600 probable breaches in eight days, having inspected 83,000 individuals under quarantine.[427] As noted by the Police Commander in Chief himself – Jaroslaw Szymczyk – this amounted to a fraction of 1%.[428] Non-compliance thus does not appear to have been a major issue in Poland under the former system.

In this context, the creation of an App requiring users to provide facial images for biometric processing – coupled with the threat of criminal sanctions on those who fail to install it – appears to be both an unnecessary and disproportionate means to ensure compliance with self-isolation requirements.

If the objective of the home quarantine app is to improve the efficiency of regulating self-isolation compliance, a discretionary app in which a large segment of citizens voluntarily provides their data is still likely to meet this objective (unlike in the app that was deployed, which was mandatory and thus gave citizens no choice whether to submit their biometric data).

A mandatory app would further carry the obvious benefit of granting citizens autonomy over whether they submit their biometric data to the state, and as such would strike a better balance between the individual right to privacy and the wider public health interest.

Alternatively, the use of high financial penalties and an advertising campaign are also likely to have met this objective and would arguably be a more proportionate response than a compulsory app given the low rates of non-compliance. Furthermore, the Panoptykon Foundation reports that individuals are still being subject to police visits, even while using the app.

This calls into question the premise under which the app was created and subsequently rendered compulsory[429] – namely, to free up police time and avoid the need for repeated home visits.

A further concern is the length of time that the biometric data is held. While the Minister stored personal data for 6 years from the point at which an account is deactivated, this general rule does not apply to photos, which are instead deleted when the user's account is deactivated.[430]

While it is *prima facie* positive that biometric data is treated differently from other non-biometric personal data, it is worth questioning whether the retaining of biometric data until the user's account is deactivated is necessary, given the burden which that puts on the citizen to ensure that their right is realised, especially when the "task" of verifying compliance is completed moments after a photograph is submitted for processing.

Such questions carry particular pertinence in light of Recital 39 GDPR, which requires that "the storage period [of personal data] is limited to a strict minimum".

### 2.2.3 Government Motivations for Biometric Surveillance

Initially, the Home Quarantine app was introduced as a voluntary tool, with the Ministry of Digitalisation making representations that it did not intend to make the app compulsory.[431]

However, by March 31st – a few weeks after its initial launch – the app became compulsory for all users.[432] This appears a common trait of the surveillance creep engendered by the roll out of biometric surveillance technologies in other countries where they are often introduced purportedly as temporary trials but then become permanent fixtures.

This sudden change raises questions as to whether the justifications under which the app was created - namely, to be a discretionary app seeking to improve the cost and efficacy of overseeing self-isolation compliance - were genuine and transparent.

---

420 **See supra** (n19).
421 **Article 9 GDPR.**
422 **Panoptykon Foundation, 'Aplikacja „Kwarantanna domowa" – obowiązkowe nie oznacza skuteczne' (31 March 2020)** https://panoptykon.org/aplikacja-kwarantanna-domowa-obowiazkowa-krytyka
423 **Hariz Baharudin and Lester Wong, 'Coronavirus: Singapore develops smartphone app for efficient contact tracing' (the Straits Times, 20 March 2020)** https://www.straitstimes.com/singapore/coronavirus-singapore-develops-smartphone-app-for-efficient-contact-tracing
424 **Hannah Beech, 'Tracking the Coronavirus: How Crowded Asian Cities Tackled an Epidemic', (NYT, 21 April 2020)** https://www.nytimes.com/2020/03/17/world/asia/coronavirus-singapore-hong-kong-taiwan.html
425 **Gazeta, 'Rząd uruchamia aplikację Kwarantanna domowa. 20 minut na wysłanie selfie lub wizyta policji' (20 March 2020)** https://next.gazeta.pl/next/7,173953,25806038,rzad-uruchomia-aplikacje-kwarantanna-domowa-20-minut-na-wyslanie.html
426 **For example, see UK Government, 'New legal duty to self isolate comes into force today' (28 Sept 2020)** https://www.gov.uk/government/news/new-legal-duty-to-self-isolate-comes-into-force-today
427 **TVN24, 'Komendant Główny Policji: prawdopodobnie 600 przypadków niestosowania się do kwarantanny' (19 March 2020)** https://tvn24.pl/najnowsze/koronawirus-w-polsce-komendant-glowny-policji-600-przypadkow-niestosowania-sie-do-kwarantanny-4368858
428 **Ibid.**
429 **See supra** (n23).
430 **Para. 9(11) Regulations.**
431 **See supra** (n23).

It is unclear what changed so shortly after the app's launch, sufficient to prompt the government to diverge from its previous commitments and render the app compulsory.

Furthermore, even if the government's representations were genuine, the benefits of improved cost and efficiency alone do not appear to be convincing justifications for the infringement of people's fundamental rights, especially when there appears to have been little imperative to do so, and in any case significantly less intrusive alternatives are likely to have met the same objective.

### 2.2.4 Mass Surveillance Concerns

Key risks from the use of a Home Quarantine app in the biometric mass surveillance context include that photos taken for the purposes of ensuring self-isolation compliance are abused/leaked by the private company responsible for developing the app, misused by the authorities who are permitted to access them, or else may be accessible by authorities not covered in the regulations. Each point shall be addressed in turn.

First, the Home Quarantine app was developed by a private company, TakeTask, in a mere three days.[433]

Given this short time frame, questions have been raised as to whether the app has been adequately means-tested to ensure the personal and biometric data of app users is completely secure against potential data breaches.

This is particularly pertinent, given that thousands of Polish citizens have or are using the application.[434] CEO Marek Mróz has sought to alleviate security concerns, pointing out that the biometric data garnered is stored on a Microsoft Azure server and that the system underwent testing by Poland's special services prior to its launch.[435]

However, there are questions as to whether the Microsoft Azure server can be 100% secure, a particular concern given the likely quantity and sensitivity of the biometric data held on the server. Furthermore, there appears to be little information indicating whether the testing conducted by Poland's special services was open source.

It is also worth noting that, as per para. 9 s. 4 of the App Regulations, TakeTask is one of the recipients of the personal data processed by the App. Since the App's purpose is to facilitate police efforts to enforce domestic quarantine requirements, it is unclear why TakeTask – a private company – is in receipt of the personal data of app users.

This is particularly significant in light of the risk that TakeTask, like other companies, may sell personal and biometric data to third parties seeking to develop or train their algorithms.

Secondly, para. 9 s. 9 of the Regulations sets out that the bodies permitted to receive the processed data – including the facial images – under para. 9 s. 4 may do so only to monitor self-isolation compliance. This provision appears to be sufficiently well-defined to avoid the risk of data being misused by the bodies set out in the Regulation.

However, in relation to access by authorities not covered by the Regulations, the Panoptykon Foundation has expressed concern that the special services – including the Internal Security Agency, Anti-Corruption Bureau, and Military Intelligence Service – are subject to almost no provisions on the protection of personal data.[436]

As a consequence, it suggests that, should photographs be intercepted by any of these organisations, they risk being used for the purposes of surveillance or of training facial recognition algorithms.

More broadly, in light of the rise in the use of biometric mass surveillance across Europe, there is a risk that such practices will equally arise in Poland.

This shift is likely to be facilitated in a context whereby citizens become accustomed to seeing their personal autonomy and right to privacy eroded or undermined.

As such, the use of a compulsory biometric app risks setting a dangerous precedent, in which respect for the sensitivity and dangers of processing biometric data on a mass scale becomes ignored in the pursuit of what is deemed convenient by the state and public authorities more generally.

---

[432] **Telepolis, 'Kwarantanna domowa będzie działać dłuzej, dodatkowo w języku rosyjskim i ukraińskim' (7th July 2020)** https://www.telepolis.pl/wiadomosci/aplikacje/kwarantanna-domowa-rok-dluzej-rosyjski-ukrainski; See *supra* (n424).

[433] **Signs, 'Twórcy aplikacji „Kwarantanna domowa" odpowiadaja na zarzuty' (17th April 2020)** https://www.signs.pl/tworcy-aplikacji-_kwarantanna-domowa_-odpowiadaja-na-zarzuty,386627,artykul.html

[434] **Polish Government, 'Ponad 10 tysiecy osób korzysta z naszej aplikacji Kwarantanna Domowa! Odpowiadamy na Wasze pytania' (23rd March 2020)** https://www.gov.pl/web/cyfryzacja/ponad-10-tysiecy-osob-korzysta-z-naszej-aplikacji-kwarantanna-domowa-odpowiadamy-na-wasze-pytania#:~:text=Ch%C4%99tnie%20na%20wszystkie%20odpowiemy!,pe%C5%82nego%20korzystania%20z%20naszej%20apki

[435] **Interia Biznes, 'Aplikacja "Kwarantanna domowa" pod lupa. TakeTask odpowiada na watpliwości branży i użytkowników' (21st April 2020)** https://biznes.interia.pl/finanse/news-aplikacja-kwarantanna-domowa-pod-lupa-taketask-odpowiada-na-,nId,4445461

[436] **See supra** (n23).

# 3. THE USE OF FINGERPRINTS IN BIOMETRIC IDS

## 3.1 The Current Law

The national identity card is one of the most important documents issued to Polish citizens.[437] All adult citizens are legally obliged to possess one.[438] Such cards are often used as identification in a variety of situations, such as for the purchase of age-restricted products, travel, or the taking out of a loan or a mortgage.

The current rules regulating the application, issuing, and use of identity cards are laid out in the Law on Identity Cards of the 6th August 2010.[439] At present, the Act makes no mention of the use of biometric data. However, a bill proposed by the Secretary of State for Internal Affairs and Administration - and recently passed by the Polish Parliament - aims to facilitate the implementation of Regulation (EU 2019/1157) by amending the 2010 Act. In doing so, it seeks to make provision for the collection and use of biometric fingerprints and facial images. This bill is known as the "draft act amending the act on identity cards and certain other acts".[440]

At present, the Polish ID card contains both a graphic layer (visible to the naked eye) and an electronic layer.[441] Art. 12(1)(g) specifies that the graphic layer shall include a facial image of the card holder. However, the 2010 Act does not classify this facial image as 'biometric data' per se. Indeed, the GDPR only classifies facial images as biometric data if subject to "specific technical processing allowing the unique identification or authentication of a natural person."[442] This usually involves using the image data to create an individual digital template or profile, which in turn is used for automated image matching or identification.

The data pertaining to each ID card, including this facial image, is permanently stored on a Register of Identity Cards.[443] It is highly concerning that such data is never deleted.[444] The Register's maintenance and development is overseen by the Minister of Computerisation,[445] who must fulfil his or her duties in compliance with the GDPR.[446] Access to this data can be obtained either through regular access or special access.

Regular access allows specified bodies to access the Register without major restrictions, including the Minister of Internal Affairs and the Minister of Computerisation.[447] Special access allows certain entities to request one-off access to the Register for a specified purpose.

A litany of bodies may make such a request, including the Chief Commandant of the Border Guard, Head of the Military Intelligence Service, Head of the Military Counterintelligence Service, Head of the Internal Security Agency, and Head of the Central Anticorruption Bureau. Special access is only granted where a request is justified by the scope of the specific tasks, alongside a series of other requirements.[448]

## 3.2 The Proposed Amendments

In this existing context, the key change proposed by the Bill is to replace Article 12a of the 2010 Act with a new list of the data included in the electronic layer of the ID.[449] Included in this list is the storage of biometric data in two forms: a face image and fingerprints.

The novel change is the inclusion of fingerprints, a form of biometric data wholly absent from the original text. Additionally, while the inclusion of a facial image is not new (and indeed is a common feature of most IDs), the fact that the bill seeks to categorise facial images as biometric data could be indicative of two things. It could suggest facial images were always subject to "specific technical processing", and thus the bill seeks to update the 2010 Act to ensure its compliance with the GDPR.

Alternatively, it could be an indication of the way the Polish authorities intend to use such data for specific technical processing in future.

---

437 **Ministry of Digitalisation, 'Dowód osobisty — informacja o dokumencie' (6 March 2019)** https://obywatel.gov.pl/pl/dokumenty-i-dane-osobowe/dowod-osobisty-informacja-o-dokumencie

438 **2010 Act Art. 5 para. 2.**

439 **Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych Dz. U. 2010 Nr 167 poz. 1131 [Act on Identity Cards] ["2010 Act"] (Dz. U. 2010, iten 1131)** http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101671131

440 **Projekt ustawy o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw [Draft act amending the act on identity cards and certain other acts]** ["Draft Bill"].

441 **2010 Act Art. 11** para. 1.

442 **GDPR Recital 51.**

443 **2010 Act Art 56.** Paras. 1-3.

444 **2010 Act Art. 56.2.**

445 **2010 Act Art 55(2).**

446 **2010 Act Art 52.8.**

447 **2010 Act Art. 55.7.**

448 **2010 Act Arts. 66.2(1), 66.2(2), 66(3).**

The bill further clarifies the only individuals exempt from the requirement to provide fingerprints as part of the ID application process are those persons:
1.a under the age of 12;
1.b from which it is temporarily physically impossible to take prints of any of the fingers;
1.c from which taking fingerprints is physically impossible.[450]

All three grounds for exemption are highly limited in scope. In addition, the first two grounds only offer a temporary exemption (the exact meaning of the second option is highly ambiguous). It can thus be inferred the vast majority of Polish citizens will be legally required to provide their fingerprints at some point in their lives.

The bill seeks to amend Article 59[451] by including "fingerprints" among the list of data stored in the Register of Identity Cards. However, it stipulates that fingerprints shall be stored on the Register: a) for no longer than 90 days after the ID card has been issued; b) until the application for an ID card has been left without examination; or c) until the administrative decision referred to in Art. 32.[452] However, it is worth noting that – with the exception of fingerprints – the data collected in the Registry is not deleted.[453]

As a consequence, it can be assumed that facial images, despite being classed as biometric data under Art. 1 para. 4(a)(1) of the draft bill, are to be held in the Registry of Identity Cards indefinitely.

The bill seeks to insert a new provision – art. 12ca[454] - which stipulates the entities who may access the biometric fingerprint data contained in the electronic layer of the ID card. These entities are cited as those referred to in art. 66 s. 3 points 1-11 of the 2010 Act and include: the Public Prosecutor's Office; Head of the Military Intelligence Service; Head of the Military Counterintelligence Service; Head of the Internal Security Agency; Head of the Foreign Intelligence Agency; and the Head of the Central Anticorruption Bureau.

### 3.2.1 Inability to Consent

In Poland, it is compulsory for all citizens to possess a national identity card – a situation in line with 14 other EU Member States. This legal position distinguishes the nature of ID cards from passports,[455] which are not a legal requirement in Poland. Under the proposed ID Bill, a citizen's failure to submit their fingerprints will result in the relevant commune authority refusing to provide them with an ID card.[456]

This provision, in turn, will prevent citizens from meeting their legal obligation to possess a card under the 2010 Act.

Thus, the interaction of the ID bill with the pre-existing domestic law leads to the creation of a chain of statutory obligations on the private citizen; a chain which – ultimately - deprives citizens of all discretion or autonomy in choosing whether to submit their fingerprints, effectively removing their ability to genuinely consent to processing of their biometric data.

In Michael Schwarz v Stadt Bochum,[457] the CJEU held that citizens could not be seen to have consented to the collection of their biometric data when this is the only way to access a service.[458] While the case of Schwarz found such collection was necessary and proportionate in the instance of passports, it is unclear that this rule extends to National IDs, for the reasons discussed below.

### 3.2.2 Necessity and Proportionality

The introduction of compulsory biometric IDs has been justified by the European Commission – and in turn the Polish government – through the need to better protect national security and better facilitate freedom of movement.[459]

In the case of *Michael Schwarz v Stadt Bochum*, the CJEU found that the compulsory taking of fingerprints for passports was proportionate to meet the objective of protecting against the fraudulent use of passports. However, the use of passports can be differentiated from national IDs.

Firstly, as previously mentioned, national IDs are compulsory in Poland. The EU's own Impact Assessment on its ID Regulation suggested this may mean the necessity test for collecting biometric data in the instance of national IDs is higher than passports.[460]

Secondly, there is arguably a mismatch between the key justifications for introducing compulsory biometric IDs – namely, better safeguarding national security and facilitating freedom of movement – and the reasons for which IDs are often used by citizens. Identity cards can only be used primarily inside the EU by individuals exercising their right to free movement.

Such travel documents are not routinely checked in the internal borders of the Union because of the principles of mutual trust and mutual recognition underpinning the framework of the Schengen agreement, and the cooperation between Member States in the area of freedom, security, and justice in general.

Furthermore, the majority of EU citizens tend not to use the ID card for cross-border travel but rather for other civic purposes. As such, they suggest there is a mismatch between the intention to improve security and facilitate freedom of movement and the legal and practical purposes for which the ID cards are used.

This mismatch, in the context of a potentially heightened necessity test given the compulsory nature of national IDs, raises questions as to whether the Regulation – and in turn, Poland's domestic Bill – are strictly necessary.

Thirdly, the ID Bill shall require the use of two types of biometric data – namely, biometric facial images and fingerprints. The EU's Impact Assessment on the Regulation suggested that while facial images should be mandatory, fingerprints should be merely optional.[461] It is unclear why the Commission decided to override this advice, especially given the limited role identity cards play in cross-border travel as covered above, and instead decided to use two types of biometric data.

Fourthly, Art. 1 para 4(b)of the ID Bill could be a cause for concern by making the collection and processing of fingerprints compulsory for any Polish child aged 12 or above. It is unclear why recording the fingerprints of children at such a young age is deemed necessary, given the seemingly remote chance that a child aged 12 shall pose a security threat sufficient to warrant the taking of their fingerprints.

Neither the Commission, nor Poland's Draft Bill nor White paper, provide an explanation as to why the age has been set at 12. It is further worth noting that the personal data of children enjoys a higher level of protection under EU law, and thus processing of such sensitive data should be adequately justified, and in any event limited to what is strictly necessary for the purpose of national security.

### 3.2.3 Mass Surveillance Concerns

A key concern in the surveillance context is whether the biometric data stored on the IDs may be used for mass surveillance purposes. While Art. 12ca points to the authorities who may access fingerprint data, the bill doesn't explicitly state whether these entities may only access the biometric data via the Register of Identity Cards (in which case fingerprint data shall only be available for 90 days),[462] or whether they may access them independently of the Register.

If the latter, it could be inferred a second database may exist to store the biometric data contained in Poland's national ID cards.

As such, there appears to be a statutory loophole that could, theoretically, provide a basis for public bodies to collect and process biometric data for surveillance purposes.

Secondly, Art. 25(b), while imposing time limitations on the storage of fingerprints in the Register, is silent on the storage of facial images, despite classifying such images as biometric.

This creates a second statutory loophole, in which facial images, despite being upgraded from personal data to biometric data under the bill, nonetheless appear to be subject to the same data retention provisions as they were in the original Act, i.e. permanently included on the register.

This risks providing a wide array of authorities with access to these photos via the Register of ID Cards under Art. 12ca. This, in turn, creates a further risk that stored biometric images could be taken and used for the purpose of surveillance in the future.

449 **Draft Bill Art. 1 para. 4(a)(1).**
450 **Draft Bill Art. 1 para 4(b).**
451 **Draft Bill Art. 25(a).**
452 **Draft Bill Art. 25(b).**
453 **Draft Bill Art. 25(b).**
454 2010 Act Art. 1 para. 5.
455 **Neurotechnology, 'Verifinger Case Study: Polish Biometric Passport System' (2009)** https://www.neurotechnology.com/download/CaseStudy_Poland_Biometric_Passport_System.pdf
456 **ID Bill s. 29e(2).**
457 **(2013) C-291/12.**
458 **Ibid para 32.**
459 **Centre for Strategy and Evaluation Services,** 'Study to Support the Preparation of an Impact Assessment on EU Policy Initiatives on Residence and Identity Documents to Facilitate the Exercise of the Right of Free Movement' (28 Aug 2017) p i.
460 **Ibid. pg. 162.**
461 **Ibid.**
462 **Draft Bill Art. 25(b).**

# 4. PEGASUS SPYWARE

## 4.1 An overview

In 2016, The Citizen Lab – a Canadian research NGO – discovered that award-winning human rights activist, Ahmed Mansoor, had been targeted by a surveillance software developed by NSO Group, a company based in Israel.[463] Following this discovery, The Citizen Lab published a report, "Hide and Seek", which located the software in 45 countries, including Poland.[464]

This report triggered speculation that Poland's Anti-Corruption Bureau ("CBA") purchased the spyware.[465] Such speculation, coupled with an ambivalent response from Poland's government, raises questions as to the strong likelihood that the software has been used to collect the personal data – including biometric data - of citizens by the Anti-Corruption Bureau.

*Pegasus* was first developed by NSO Group Technologies, an Israel-based technology firm founded by ex-members of Unit 8200, the Israeli Intelligence Corps unit responsible for collecting signals intelligence.[466] According to its website, the company "creates technology that helps government agencies prevent and investigate terrorism and crime".[467]

The Israeli government deems the capabilities of Pegasus to be so powerful that it classifies the system as 'a weapon'.[468] Pegasus operates as a modular malware capable of conducting total surveillance on the targeted device.

Once a user's device is infected, almost all their personal data is compromised.[469] Furthermore, the programme can access to a user's microphone and video camera[470] - tools which, in turn, could open the door to biometric data processing through the use of face and voice recognition.

The programme allows the operator to freely modify the phone settings and can infect a phone without any necessary action on the part of the device user.[471]

*Pegasus* has a 'self-destruct' mechanism if it believes it has been discovered, whereby it erases itself.[472] This may occur, inter alia, where a user attempts to back-up a device.[473] *Pegasus* will automatically self-destruct if it hasn't received any communication from the operator's server in 60 days.[474]

Upon discovering Pegasus, The Citizen Lab conducted a global DNS Cache Probing study, which sourced five European operators.[475] One of these operators, ORZEBIALY, appeared to have been active in Poland from November 2017 onwards.[476] Its presence was detected in seven Polish networks.[477] Such findings suggest that Pegasus has been widely deployed within Poland to date.

Soon after The Citizen Lab's discovery, it transpired that, in September 2018, Poland's Audit Office[478] conducted an audit of the finances of the Crime Victims Assistance Fund[479] - a fund intended to help crime victims.[480] During its review, Poland's Audit Office encountered an unaccounted-for PLN 25 million payment transferred from the Fund to the Anti-Corruption Bureau.[481]

It was soon after the discovery of this suspicious invoice that The Citizen Lab detected the presence of Pegasus in Poland.[482]

Later that year, private broadcaster TVN24 released a report – 'Black and White' - suggesting the money transferred to the CBA went towards the purchase of a "*new system of spy on telephones and computers,* the most expensive system in the history of Poland's secret services"[483] - in other words, *Pegasus*. The report suggested the amount spent by the CBA was in line with the value of the Pegasus technology.[484]

The responses from high-profile political actors to these allegations have been ambiguous. Prime Minister Mateusz Morawiecki, upon being asked whether *Pegasus* had been purchased by the CBA during a press conference, responded that everything will be revealed "in due course".[485]

Since then, Morawiecki has revealed nothing further on the matter. Meanwhile, Deputy Prime Minister Jacek Sasin suggested he did not know if Poland had purchased the system, but that, in any case, "honest citizens" would have nothing to worry about.[486]

The CBA itself responded to the TVN24 Report by claiming it did not purchase any mass surveillance system to monitor the activities of citizens.[487]

However, it is worth noting the *Pegasus* system is not generally a system of mass – but targeted – surveillance. As such, this statement, even if true, constitutes a somewhat indirect refutation of the accusations levied against the CBA.

In contrast, the National Prosecutor's Office did not deny that *Pegasus* is being used by Poland's special services. Instead, it maintained that there are rules in Poland allowing for the use of *Pegasus* through Art. 19(6) of the Law on the Police of April 6, 1990.[488]

463 **Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, 'Hide and Seek' (CitizenLab, 18 Sept 2018) pg. 8,** https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries

464 **Ibid.**

465 **TVN24, 'Czarno na białym: Oprogramowanie Pegasus' (28 Aug 2019), available at** https://tvn24.pl/go/programy,7/czarno-na-bialym-odcinki,11367/odcinek-50,S00E50,95066

466 **BBC News, 'NSO Group: Israeli firm 'impersonated Facebook to spread spyware" (21 May 2020)** https://www.bbc.co.uk/news/technology-52758784

467 **NSO Group,** https://www.nsogroup.com

468 **Mehul Srivastava and Tom Wilson, 'Inside the WhatsApp hack: how an Israeli technology was used to spy' (Financial Times, 30 Oct 2019)** https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229

469 **Ibid.**

470 **See supra (n84)** pg. 7.

471 **Ibid.**

472 **Patrick Howell O'Neill, 'Inside NSO, Israel's billion-dollar spyware giant' (MIT Technology Review, 19 Aug 2020)** https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights

# 4.2 Legal Analysis

## 4.2.1 Surveillance Oversight

In Poland, there is no independent oversight body for the surveillance operations of the special services[489] analogous to the Investigatory Powers Tribunal in the UK, or the Oversight Committee for the Intelligence and Security Services or Data Protection Authority in the Netherlands.

The absence of such an oversight body in Poland, alongside a perceived lack of safeguards, led Poland's Constitutional Court in its Judgement of 30th July 2014 (Case No. K23/11) to deem that Poland's pre-existing surveillance framework violated the country's constitution – specifically the right to the protection of privacy under Article 47 and the right to protection of privacy of communication under Article 49.

The Court recommended that an independent oversight body be established, that individuals subject to surveillance be notified, and that procedural safeguards for secret surveillance be tightened.[490]

To implement this judgement, the ruling Law and Justice Party has implemented two Acts: The Act of 15th Jan 2016 on the Amendment to the Police Act and Certain Other Acts;[491] and the Act of 10th June 2016 on anti-Terrorist Activities.[492]

However, neither Act created an independent oversight body as envisioned by the Constitutional Tribunal. Furthermore, the *Police Act 2016* has been widely criticised domestically and internationally for expanding police surveillance prerogatives, as opposed to cutting them back.[493]

The *Anti-Terrorism Act 2016* has prompted similar concerns from, among others, Poland's Human Rights Ombudsman,[494] and the Panoptykon Foundation,[495] a Polish human rights NGO. Thus, there appears to be no supervisory authority in Poland with the power to regulate the potential use of Pegasus by the CBA.

Poland has also incorporated EU Directive 2016/680 - which seeks to place limits on the processing of natural persons' data for the purposes of the preventing, investigating, detecting, or prosecuting criminal offences - into domestic law via the Act of 14 December 2018 on the protection of personal data processed in connection with the prevention and combating of crime.[496]

However, this Directive has been incorporated so as not to apply to the statutory tasks conducted by the Internal Security Agency, the Foreign Intelligence Agency, the Military Counter-Intelligence Service, and - crucially - the Central Anticorruption Bureau.[497] Thus, the 2016 Directive has been implemented in a way that precludes it from regulating the potential use of Pegasus by the CBA.

### 4.2.2 The Inadequacy of Domestic Law

Poland's domestic legal framework contains no singular or coherent regulatory regime for a programme with the capabilities of *Pegasus* i.e. a programme that can compromise *all* data present on one's mobile device. Chapter 26 of the Code of Criminal Procedure 1997[498] regulates wiretapping and recording of telephone or online communications via other technical means.[499]

As such, the Code covers *some* of the capabilities possessed by *Pegasus*. However, many of the spyware's core functions, including those that could potentially lead to a large-scale gathering of biometric data, are outside the regulatory oversight of the 1997 Code. This raises issues concerning the legality of using techniques as well broader concerns for the rights to privacy, dignity, and other fundamental universally recognized human rights detailed elsewhere in this Report.

Furthermore, the laws regarding the admissibility of evidence are also found in the 1997 Code. When the code was first passed, it prohibited the taking and use of evidence obtained for the purposes of criminal proceedings by means of a prohibited act (so called '*fruit of the poisoned tree*' evidence).

However, in 2016, Poland's ruling Law and Justice Party ("PiS") introduced a series of amendments to the Code of Criminal Procedure.[500] Among these amendments was the insertion of Article 168a of the Criminal Code, which repealed the old rule preventing the admission of illegally obtained evidence.[501]

The new provision sets out that "evidence cannot be considered inadmissible solely on the grounds that it was obtained in breach of the provisions of the procedure or by means of a prohibited act referred to in Art. 1 of the Criminal Code, unless the evidence was obtained in connection with the performance of official duties by a public official as a result of: murder, wilful damage to health or imprisonment".[502]

The new provision means that, regardless of the legality of Pegasus under Polish domestic law, evidence obtained from it may be used in criminal proceedings. This was seen in the case of Slawomir Nowak, a Polish politician who is facing anti-corruption charges following evidence allegedly garnered via Pegasus.[503]

---

**473** **Ibid.**
**474** **Ibid.**
**475** **See supra (n84).**
**476** **Ibid.**
**477** **See supra (n84)** Table 6.
**478** **"Najwyższa Izba Kontroli" or "NIK".**
**479** **"Funduszu Pomocy Pokrzywdzonym".**
**480** **NIK, "Assistance to crime victims as part of the Victims' Aid Fund"(2016-2017)** https://www.nik.gov.pl/plik/id,17115,vp,19675.pdf
**481** **TVN24, 'Czy CBA ma narzędzie totalnej inwigilacji? "Infrastruktura systemu powiazana z Polską"' (29 Aug 2019)** https://tvn24.pl/polska/system-pegasus-i-pytania-do-cba-czarno-na-bialym-ra964972-2312092
**482** **Ibid supra** (n86).
**483** **Wojciech Kość, 'Poland's PiS faces questions over Israeli Spyware' (Politico, 6 Sept 2019)** https://www.politico.eu/article/poland-pis-israeli-spyware-questions
**484** **Ibid.**
**485** **Ibid.**
**486** **Ibid.**
**487** **Do Rzeczy, 'CBA inwigiluje Polaków przez program Pegasus? Biuro dementuje', (4 Sept 2019)** https://ziemkiewicz.dorzeczy.pl/kraj/112878/cba-inwigiluje-polakow-przez-program-pegasus-biuro-dementuje.html
**488** **See supra** (n102).
**489** **Dorota Głowacka and Adam Ploszka, 'National intelligence authorities and surveillance in the EU:** Fundamental rights safeguards and remedies', Helsinki Foundation for Human Rights, para. 7.
**490** **Barbara Grabowska-Moroz, 'The Polish surveillance regime before the ECHR' (about:intel, 27 April 2020)** https://aboutintel.eu/echr-poland-surveillance
**491** **Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw [Act amending the Act on the Police and certain other acts]** (Dz. U. 2016, item. 147).
**492** **Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych [anti-Terrorism Act]** (Dz. U. 2016, item 904).

### 4.2.3 Mass Surveillance Concerns

Although the *Pegasus* spyware is generally used for targeted surveillance, it also carries the potential to be used in the mass surveillance context. Almost every Polish citizen owns a smartphone.

Thus, the number of individuals potentially vulnerable to *Pegasus* is significant. It is also worth noting that targeted surveillance comes with many of the same threats to individual rights and freedoms as mass surveillance (e.g. of discrimination) and that its arbitrary use against individuals can nevertheless create a perception of mass surveillance.

While, according to the NSO Group website, *Pegasus* is intended to aid governments in tackling public security threats, the programme is reported to have been used as a tool by governments to engage in the suppression of public dissent. In 2012, a contract worth $2 million was signed between NSO Group Technologies and the Mexican government, which the Mexican state allegedly used to engage in the surveillance of journalists and human rights activists.

Its use has also been linked to the killing of Saudi dissident Jamal Khashoggi,[504] and the tracking of Rwandan political dissidents in the UK.[505]

Given such a record, it is concerning that *Pegasus* may have been purchased by the CBA, without public knowledge and, as discussed above, with little oversight.

The wide spectrum of capabilities of Pegasus, and accordingly the possibility of it being involved in widespread biometric mass surveillance (via either indiscriminate surveillance or arbitrarily-targeted surveillance), creates further concerns regarding a possible mismatch between the legal remit of the CBA and the intended use of Pegasus, especially in the light of Art 7 of the Polish Constitution.[506]

---

493 **Amnesty International, 'Poland: New surveillance law a major blow to human rights' (29 Jan 2016)** https://www.amnesty.org/download/Documents/EUR3733572016ENGLISH.pdf; Panoptykon Foundation, 'No control over surveillance by Polish intelligence agencies: ECHR demands explanation from the government' (18 Dec 2019) https://en.panoptykon.org/government-surveillance-echr-complaint; Rojszczak, M., 'Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland' Democracy and Security (2021) 17(1).

494 **Ombudsman, 'Apel RPO do Prezydenta w sprawie ustawy antyterrorystycznej' (21 June 2016)** https://www.rpo.gov.pl/pl/content/apel-rpo-do-prezydenta-w-sprawie-ustawy-antyterrorystycznej

495 **Panoptykon Foundation' 'Poland adopted controversial anti-terrorism law' (22 June 2016)** https://en.panoptykon.org/articles/poland-adopted-controversial-anti-terrorism-law

496 **Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestepczości [Act on the Protection of Personal Data}** (Dz. U. 2019, item 125).

497 **Ibid.**

498 **See supra** (n22).

### 4.2.4 Human Rights Concerns

While the courts and prosecutors may step in to scrutinise the activities of Poland's secret services, a person subject to surveillance is usually denied access to information gathered about them during the surveillance period.[507]

This is often justified on the basis of a lack of a legal requirement to notify individuals that they are the target of surveillance (contrary to the 2014 judgement of the Constitutional Tribunal and ECHR law[508]). Alternatively, a certain entity is refused a right to know the statistics of surveillance due to, for instance, a tense international situation.

As a consequence, given most targets are never notified that they are under surveillance, they are unable to enforce their constitutional and European rights before Poland's domestic courts.

The concerns around the limited access to judicial recourse are compounded by the lack of an oversight body to ensure the legal compliance of surveillance operations.

At present, Poland does not possess an independent oversight body related to the conduct of its secret services, akin to the Investigatory Powers Tribunal in the UK.

---

499 **Article 237(1) of the Code of Criminal Procedure 1997 allows the secret services to wiretap, but only a) when the court has granted its consent; and b) only in relation to pending proceedings or to prevent the commission of a new offence. Such a request may only be made in relation to the gathering of evidence for a fixed list of offences, as per Art 237(3).**

500 **Aleksandra Rychlewska, 'O PRZEPISIE ART. 168A K.P.K. JAKO PRZYZWOLENIU NA KORZYSTANIE W RAMACH PROCESU KARNEGO Z DOWODÓW ZDOBYTYCH W SPOSÓB NIELEGALNY' (Palestra, May 2016)** https://palestra.pl/pl/czasopismo/wydanie/5-2016/artykul/o-przepisie-art.-168a-k.p.k.-jako-przyzwoleniu-na-korzystanie-w-ramach-procesu-karnego-z-dowodow-zdobytych-w-sposob-nielegalny

501 **Ibid.**

502 **See supra (n22) Art. 168a.**

503 **Monika Kamińska, Joanna Potocka, 'Nowak wpadł przez system Pegasus? Budka żąda wyjaśnień ws. inwigilacji opozycji' (RMF24, 23 July 2020)** https://www.rmf24.pl/fakty/polska/news-nowak-wpadl-przez-system-pegasus-budka-zada-wyjasnien-ws-inw,nId,4627304; **Wprost, 'Sprawa Nowaka pretekstem do inwigilacji sztabu Trzaskowskiego? Kamiński odpowiada na tezy Budki' (23 July 2020)** https://www.wprost.pl/kraj/10346788/sprawa-nowaka-pretekstem-do-inwigilacji-sztabu-trzaskowskiego-kaminski-odpowiada-na-tezy-budki.html

504 **David Kirkpatrick, 'Israeli software helped Saudis spy on Khashoggi, Lawsuit Says' (NYT, 2nd Dec 2018)** https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html

505 **See supra (n89).**

506 **Article 7 of the Polish Constitution sets out that "the organs of public authority shall function on the basis of, and within the limits of, the law".**

507 **Ustawa o policji [Act on the Police]** (Dz. U. 1990, item 179) Article 19.16.

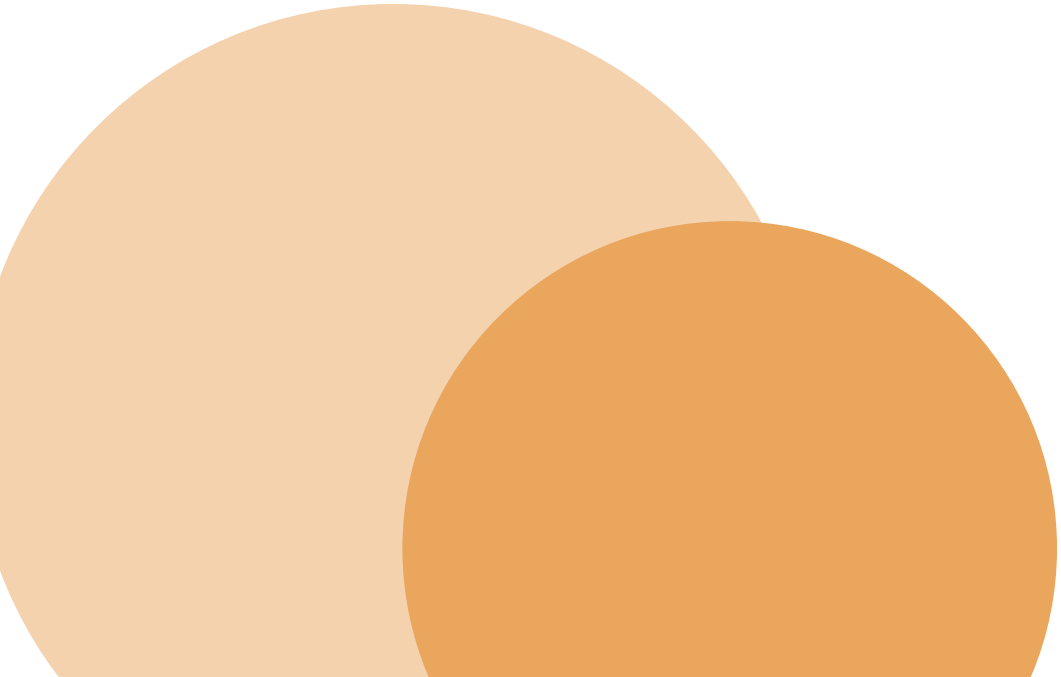
508 **Zakharov v Russia App no 47143/06** (ECHR, 28 March 2007).

509 **Including: the Sejm and the Sejm Committee on Special Services, Supreme Audit Office, Human Rights Ombudsman, State Government Bodies, Courts and Prosecutors, the Internal Oversight Bureau of the Ministry of the Interior and Administration.**

This is in contrast to 21 of the EU's 27 Member States, and despite a 2014 ruling by the Polish Constitutional Tribunal, which found that the operations of the country's secret services required such oversight.

Instead, Polish law contains a patchwork of parliamentary, judicial, and administrative bodies[509] who are capable, to a greater or lesser degree, of overseeing the activities of Poland's secret services - including the CBA. However, the remit and effectiveness of these bodies is limited.

The Sejm Committee on Security Service primarily consists of parliamentarians belonging to Poland's governing Law and Justice Party. Therefore, its robustness and independence may be called into question, especially in the light of suggestions that there is a wider degradation of the rule of law in Poland.



# 5. CONCLUSION

**At present, the prevalence of biometric mass surveillance practices in Poland appears to remain comparatively low. However, the appearance of biometric systems such as Pegasus and the Home Quarantine App risks functioning as a stepping stone, opening the door to biometric mass surveillance in the future. The biometric mass surveillance infrastructures created by compulsory national biometric IDs further compounds these risks.**

Biometric data is often gathered and processed in the name of convenience, justified by the need to improve the efficiency with which public policy objectives are met, and dismissed as the natural consequence of technological development.

This reasoning underpins the inclusion of fingerprints in the digital layer of identity cards and the Home Quarantine app.

However, the risk of data spilling beyond its intended confines – and being accessed by various public authorities without proper judicial and administrative oversight or a concrete legal basis – is often overlooked in these situations. Poland's domestic framework for the processing of biometric data is unclear and often outdated.

Beyond the GDPR, there is scant domestic legislation regulating its use. This is likely to become increasingly problematic, given the rising use of biometric processing by Poland's public authorities.

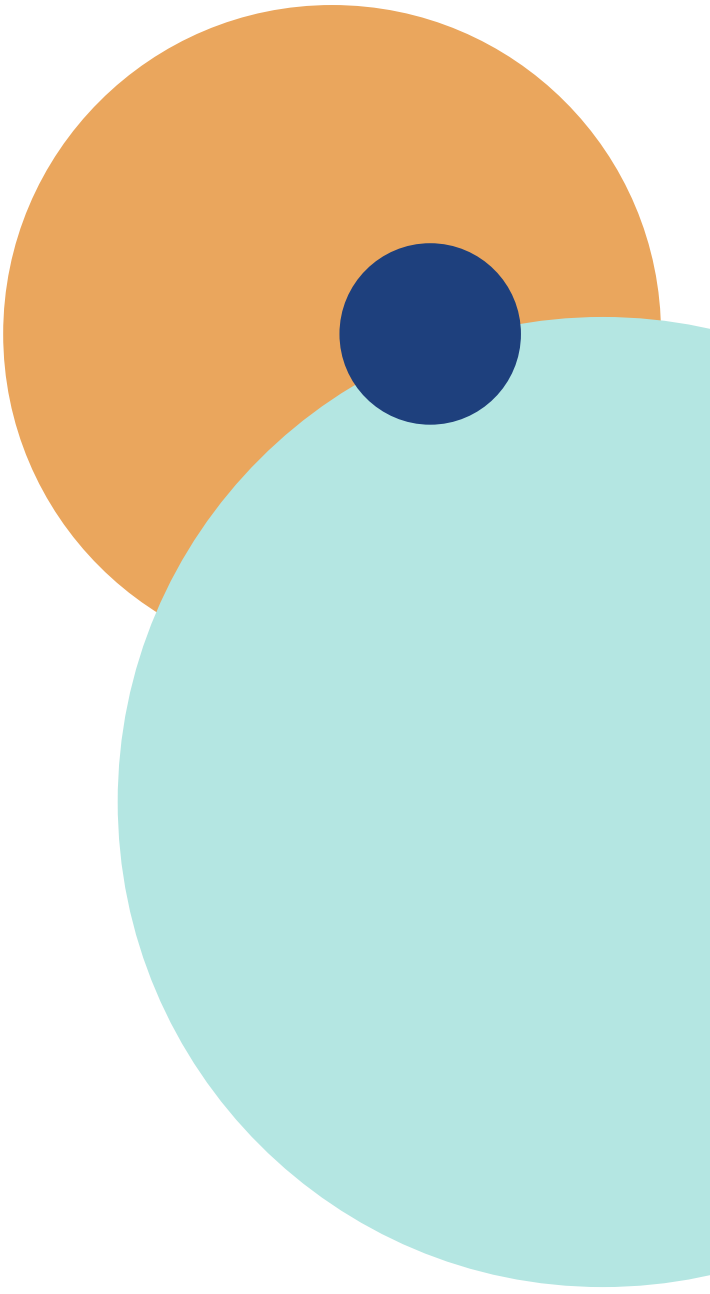
Since the deployments identified by this report have yet to evolve into full-scale remote biometric identification, Poland now appears to sit at a crossroads.

It could, on the one hand, strengthen its domestic legal regime governing the use of biometric data, while ensuring the UODO continues to address privacy shortcomings.

This would likely reduce the risk of current deployments morphing into biometric mass surveillance practices of the kind and extent seen in the Netherlands and Germany.

Conversely, the maintenance of the status quo risks leading to the normalisation of biometric processing within Polish society, providing a social and legal climate in which biometric data could be used for general surveillance purposes in the future.

The Home Quarantine App and ID Bill – and, notably, the CBA's likely purchase of Pegasus spyware – point to the latter scenario being more likely. Should this possibility materialise, Poland will join a litany of other European states in conducting systemic biometric mass surveillance of people in public and publicly-accessible spaces. This is a particularly troubling development in a country which is currently witnessing a wider degradation in the rule of law.



# GENERAL SUMMARY

**The use of biometric mass surveillance in public spaces has increasingly, and quietly, become regular practice in recent years. This report examines various case studies of biometric mass surveillance, in varying levels of detail, as deployed in three EU member states: Germany, the Netherlands, and Poland. Each instance was examined by reference to domestic, European, and, where appropriate, international legal principles.**

In regard to Germany, examples of biometric mass surveillance remain despite an otherwise strong culture of privacy protection and respect for the rule of law. These involve the use of facial recognition in public spaces, where a market involving collaborations between private and state authorities appears to have extended the use of biometric mass surveillance beyond its purported remit.

An increased reliance on mass biometric processing also took other forms, notably the soon-to-be mandatory inclusion of fingerprint data on state ID cards which raises concerns regarding consent and access extension, among others. Efforts to protect young people have also increased reliance on biometric data that may pose risks for adults seeking to access services that previously did not rely on the mass collection of biometric data.

Finally, measures implemented in the course of the COVID-19 pandemic appear to have created a new frontier for biometric mass surveillance, with issues focusing on the longevity and necessity of such measures.

Examples of biometric mass surveillance have also been identified in the Netherlands, uses which are also often characterised by unsubstantiated legal bases and an overall lack of transparency. Uses of biometric mass surveillance in the Netherlands arise from public and private bodies, as well as collaborations between both sectors. In regards to public bodies, the report examines the use of facial recognition technology, notably the use of the 'CATCH' database by law enforcement.

Private actors have also been deploying biometric mass surveillance practices, for example in retail and stadiums, with little or ineffective oversight by the relevant DPAs.

Finally, the public-private collaborative use of 'Living Labs', which process biometric data obtained in public spaces for experimental reasons, was also noted as a particularly intrusive example that raises concerns in regard to proportionality and respect for human dignity.

In Poland, we found that the use of biometric mass surveillance has been on the rise in the past five years. Three instances were identified.

The first was the operation of the compulsory Home Quarantine App, which processes the biometric data of its users to monitor compliance of self-isolation requirements. Secondly, the report examined the proposed bill seeking to make the collection and processing of biometric data compulsory on national ID cards.

The final instance is the likely purchase of the spyware software 'Pegasus' by Poland's anti-corruption bureau, which could open the door to mass biometric surveillance via nonconsensual access to citizen's mobile phones.

Across all three countries, several instances of biometric mass surveillance have been characterised as 'tests' or 'trials' and appear to have evaded closer scrutiny due to their temporary nature.

Other instances also highlight what could be considered an underwhelming response by relevant Data Protection Authorities ('DPA'), with examples of slow responses and restricted remedies having been identified.

This points towards an open-ended use of biometric mass surveillance, whereby it is deployed less in response to specific and evidentiary threats but rather indiscriminately as a precautionary or deterrent measure.

In our analysis, such practices consistently engage (and fail to comply with) principles of necessity and proportionality found in both domestic and European legal frameworks, as well as having deeper implications for the right to dignity that underpins fundamental human rights principles in Europe and beyond.

# BIBLIOGRAPHY


## Journals and Reports

**Amnesty International,** 'Kabinet, voorkom toeslagenaffaire in het kwadraat' Nieuws (18 January 2021) available at: https://www.amnesty.nl/actueel/kabinet-voorkom-toeslagenaffaire-in-het-kwadraat

**Amnesty International,** 'Poland: New surveillance law a major blow to human rights' (29 Jan 2016) https://www.amnesty.org/download/Documents/EUR3733572016ENGLISH.pdf

**Article 29 Data Protection Working Party,** Guidelines on transparency under Regulation 2016/679 (WP260 rev.01, adopted 29th of November 2017, revised 11th of April 2018) available at: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025

**Barak, A.,** Human Dignity: The Constitutional Value and the Constitutional Right (2016) Human Rights Law Review, 16(1), 156-169 https://doi.org/10.1093/hrlr/ngv042

**Centre for Strategy and Evaluation Services,** 'Study to Support the Preparation of an Impact Assessment on EU Policy Initiatives on Residence and Identity Documents to Facilitate the Exercise of the Right of Free Movement' (28 Aug 2017)

**Duff, A.** Who must presume whom to be innocent of what? (2013) Netherlands Journal of Legal Philosophy, 42(3)

**European Commission,** Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178

**European Digital Rights,** Ban Biometric Mass Surveillance (Brussels 2020), available at: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

**European Union Agency for Fundamental Rights,** 'Facial recognition technology: fundamental rights considerations in the context of law enforcement" (2019) available at https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

**Lang, M.,** Die Evaluation der Videoüberwachung in Bielefeld. Zugleich eine Erwiderung zu Quambusch. (Kriminalistik. 2005) S. 723–726

**Minaj, J., & Bonnici, J.** Unwitting subjects of surveillance and the presumption of innocence. (2014) Computer Security and Law Review, 30(4)

**Neurotechnology,** 'Verifinger Case Study: Polish Biometric Passport System' (2009) https://www.neurotechnology.com/download/CaseStudy_Poland_Biometric_Passport_System.pdf

**Panoptykon Foundation,** 'No control over surveillance by Polish intelligence agencies: ECHR demands explanation from the government' (18 Dec 2019) https://en.panoptykon.org/government-surveillance-echr-complaint

**Rhue, L.,** Racial Influence on Automated Perceptions of Emotions (November 9, 2018). SSRN: https://ssrn.com/abstract=3281765 or http://dx.doi.org/10.2139/ssrn.3281765

**Rojszczak, M.,** 'Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland' Democracy and Security (2021) 17(1)

**Sadun, E.,** Digital Video Essentials: Shoot, Transfer, Edit, Share (26 December 2006) ISBN 9780470113196.

**Surveillance Studies Network,** A Report on the Surveillance Society (2006) available at https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf

**Thielbörger, P.,** The "Essence" of International Human Rights, Germany Law Journal (2019), 20, 924-939

**VISA,** 'Goodbye, Passwords. Hello, Biometrics' (2017) https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-biometrics-payments-study.pdf

**Vodafone Institute for Society and Communications,** 'Big Data: A European Survey on the Opportunities and Risks of Data Analytics' (Vodafone, 2016) available at https://www.vodafone-institut.de/bigdata/links/VodafoneInstitute-Survey-BigData-Highlights-en.pdf

### Case Law and Court Documents

**Autoriteit Persoonsgegevens,** Recommendation z2020-01329: Advies over het concept voor Wijziging van de Vreemdelingenwet 2000 ter bestendiging van verwerking biometrie (24th of June 2020), available at: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_biometrische_gegevens_vreemdelingen.pdf

**BVerfG,** Urteil des Ersten Senats vom 15 Dezember 1983 – 1 BvR 209/83, available at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html

**BVerfG,** Urteil des Ersten Senats vom 5. Juni 1973 – 1 BvR 536/72

**C-524/06** *Huber v Federal Republic of Germany,* (CJEU, 2008) European Court Reports 2008 I-09705

**C-291/12** *Schwarz v Stadt Bochum* (CJEU, 2013) 2 C.M.L.R. 5

**C 293/12** and **C 594/12** *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (CJEU, 2014) ECLI:EU:C:2014:238

**Decision of 22 February 2008** (DIS/DEC-134/2405/08), Writing of 15 December 2009 (DIS / DEC- 1261/46988/09), Judgement of the Supreme Administrative Court of 1st December 2009 (I OSK 249/09)

**HmbBfDI,** 'Antrag auf Zulassung der Berufung §§ 124, 124a VwGO Az. 5 Bf 46/20.Z - Begründung des Antrags vom 6.2.2020' (to Hamburg Administrative Appeal Court 2020) available at https://datenschutz-hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf

**HmbBfDI,** 'Az.: 11.03-13 - Einsatz Der Gesichtserkennungssoftware „Videmo 360" Durch Die Polizei Hamburg Zur Aufklärung Von Straftaten Im Zusammenhang Mit Dem In Hamburg Stattgefundenen G20- Gipfel' (2021) available at https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

**HmbBfDI,** 'Consultation Prior To An Order Pursuant To Article 58(2)(G) GDPR' (2021) available at https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.pdf

**HmbBfDI,** 'Stellungnahme Des Hmbbfdi Vom 20. Juli 2020 Zur Zulässigkeit Der Berufung Az.: J / 11.03-13' (2020) available at https://datenschutz-hamburg.de/assets/pdf/Stellungnahme_Zulassung_Berufung_2020-07-20.pdf

**President of the UODO,** Decision (ZSZZS.440.768.2018), available at https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018

*Pretty v UK* (2002) 35 EHRR 1

**Raad van State,** Uitspraak 201601536/3/V3 en 201601554/3/V3 (Reference ECLI:NL:RVS:2020:1168; 29th of April 2020), available at: https://www.raadvanstate.nl/actueel/nieuws/@120973/201601536-3-v3-en-201601554-3-v3

*S and Marper v The United Kingdom*, Applications nos. 30562/04 and 30566/04 (ECtHR, 4 December 2008)

**Verwaltungsgericht Hamburg,** (Hamburg Administrative Court 2019) Urteil vom 23 Oktober 2019 Az. 17 K 203/19 available at https://justiz.hamburg.de/contentblob/13535554/cc5a1e8c70c95088220147f57921d22d/data/17-k-203-19.pdf

**Tweede Kamer der Staten-Generaal,** Motie van het lid Van Beukering-Huijbregts c.s. over de capaciteit bij de Autoriteit Persoonsgegevens (Motion 35570-VI-62, 26th of November 2020) available at: https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2020Z22977&did=2020D48569

**Verwaltungsgericht Köln,** (18 January 2021) Az.: 20 L 2340/19, available at http://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2021/20_L_2340_19_Beschluss_20210118.html ('20 L 2340/19')

**Zakharov v Russia** App no 47143/06 (ECHR, 28 March 2007)

## Materials from the Internet

**Aachener Nachrichten,** 'Videoüberwachung in Aachen und Düren ab 2008' (Aachener Nachrichten, 2007) https://www.aachener-nachrichten.de/nrw-region/videoueberwachung-in-aachen-und-dueren-ab-200 8_aid-27935235

**Amnesty International,** 'Kabinet, voorkom toeslagenaffaire in het kwadraat' Nieuws (18 January 2021) https://www.amnesty.nl/actueel/kabinet-voorkom-toeslagenaffaire-in-het-kwadraat

**Amnesty International,** 'Poland: New surveillance law a major blow to human rights' (29 Jan 2016) https://www.amnesty.org/download/Documents/EUR3733572016ENGLISH.pdf

**Amnesty International,** 'We Sense Trouble. [online] London: Amnesty International Ltd. https://www.amnesty.nl/content/uploads/2020/09/Report-Predictive-Policing-RM-7.0-FINAL-TEXT_CK-2.pdf?x53356

**Arensbergen, W.,** 'Agenten filmen met bodycams lastige kroegbezoekers op Stratumseind in Eindhoven' ED (2017) https://www.ed.nl/eindhoven/agenten-filmen-met-bodycams-lastige-kroegbezoekers-op-stratumseind-in-eindhoven~a3ba64c8

**Baharudin, H. and Wong, L.,** 'Coronavirus: Singapore develops smartphone app for efficient contact tracing' (the Straits Times, 20 March 2020) https://www.straitstimes.com/singapore/coronavirus-singapore-develops-smartphone-app-for-efficient-contact-tracing

**BBC News,** 'NSO Group: Israeli firm 'impersonated Facebook to spread spyware'' (21 May 2020) https://www.bbc.co.uk/news/technology-52758784

**Beech, H.,** 'Tracking the Coronavirus: How Crowded Asian Cities Tackled an Epidemic', (NYT, 21 April 2020) https://www.nytimes.com/2020/03/17/world/asia/coronavirus-singapore-hong-kong-taiwan.html

**Beuth, P.,** 'Hamburgs Datenschützer Leitet Prüfverfahren Gegen Clearview Ein' (Spiegel.de, 2020) https://www.spiegel.de/netzwelt/web/clearview-hamburgs-datenschuetzer-leitet-pruefverfahren-ein-a-0ec1870d-c2a5-4ea1-807b-ac5c385ae165

**Biometric Update,** 'Hooyu Biometrics approved in Germany' (Biometric Update, 2021) https://www.biometricupdate.com/202101/hooyu-biometrics-approved-in-germany-new-ui-tools-launched

**Boghani, P.,** 'Artificial Intelligence Can Be Biased. Here's What You Should Know.' Frontline (2019) https://www.pbs.org/wgbh/frontline/article/artificial-intelligence-algorithmic-bias-what-you-should-know

**Bouma, R. and Damen, F.,** 'Slimme deurbel rukt op in strijd tegen inbraken, maar hoe zit het met privacy?' NOS (2020) https://nos.nl/nieuwsuur/artikel/2318362-slimme-deurbel-rukt-op-in-strijd-tegen-inbraken-maar-hoe-zit-het-met-privacy.html

**BNR Webredactie,** 'Forse Toename Cameras met Gezichtsherkenning, Capaciteit AP Schiet Tekort' BNR (23 November 2020) https://www.bnr.nl/nieuws/juridisch/10426941/forse-toename-camera-s-met-gezichtsherkenning

**Brainport Eindhoven,** 'Kunstmatige intelligentie ondersteunt Stadstoezicht en politie tijdens carnaval' Nieuws (2020) https://brainporteindhoven.com/nl/nieuws/kunstmatige-intelligentie-ondersteunt-stadstoezicht-en-politietijdenscarnaval?tx_sitetemplate_newsletter%5Baction%5D=subscribe&tx_sitetemplate_newsletter%5Baction%5D=subscribe&tx_sitetemplate_newsletter%5Bcontroller%5D=Newsletter&cHash=2f458f52f458f51cd681438376affe805a74e33

**Burt C.,** 'Biometrics Industry Seeing Higher Demand And Adapting Technology To Help Outbreak Mitigation (Biometric Update, 2020) https://www.biometricupdate.com/202003/biometrics-industry-seeing-higher-demand-and-adapting-technology-to-help-outbreak-mitigation

**Cadwalladr, C. & Graham-Harrison, E.,** 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' (The Guardian, 17 March 2017) www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

**Cognitec,** 'Facing the mask challenge' (Cognitec) cognitec.com/files/tao/downloads/Cognitec-Facing-the-Mask-Challenge.pdf

Cognitec, 'FaceVACS-DVScan LE flyer', (Cognitec) https://www.cognitec.com/facevacs-dbscan-le.html

**Cognitec,** 'Facevacs-Videoscan' (Cognitec) https://www.cognitec.com/facevacs-videoscan.html

**Cognitec,** 'FaceVACS-VideoScan flyer' (Cognitec) https://www.cognitec.com/facevacs-dbscan-le.html

**Cognitec,** 'New Mask-Tolerant Matching Algorithm And Age Estimator' (Cognitec, 2021) https://www.cognitec.com/news-reader/cognitec-product-releases-2021.html

**Cognitec,** 'Partners' (Cognitec, 2020) https://www.cognitec.com/partners.html

**Crowdwatch Nederland,** various Facebook posts: https://www.facebook.com/crowdwatchnl/posts/1547482191928815 (2017), https://www.facebook.com/crowdwatchnl/posts/1664213833588983 (2017), https://www.facebook.com/crowdwatchnl/posts/2385899338087092 (2019).

**Dallmeier,** Dallmeier integrates AnyVision facial recognition into its "HEMISPHERE®" software platform for security and business (Dallmeier.com) https://www.dallmeier.com/about-us/press-centre/anyvision-facial-recognition#c1219

**Dallmeier,** 'Dallmeier Releases New Tutorial Videos On Viewing Software Smavia Viewing Client' (Sourcesecurity.com) https://www.sourcesecurity.com/dallmeier-smavia-viewing-client-cctv-software-technical-details.html

**Dallmeier,** Panomera S Series Brochure (Dallmeier) https://www.dallmeier.com/fileadmin/user_upload/PDFs/Technology/Panomera/Dallmeier_Panomera_S-Series_Brochure_EN.pdf

**Dallmeier,** Software (Dallmeier.com) https://www.dallmeier.com/technology/software

**Dermalog,** 'Retailers Rely On DERMALOG's Temperature Screening' (Dermalog, 2020) https://www.dermalog.com/news/article/retailers-rely-on-dermalogs-fever-screening

**Davis, D.,** 'Facial recognition technology threatens to end all individual privacy' The Guardian (2019) https://www.theguardian.com/commentisfree/2019/sep/20/facial-recognition-technology-privacy

**Dekker, S.,** 'Antwoord op vragen van het lid Verhoeven inzake het bericht 'Tientallen camera's houden klanten van filiaal Jumbo in de gaten: 'Willen we dit?'" Tweede Kamer der Staten-Generaal (2020) https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D01497&did=2020D01497

**Deutsche Welle,** 'Germany's Facial Recognition Pilot Program Divides Public' (Deutsche Welle, 2017) https://www.dw.com/en/germanys-facial-recognition-pilot-program-divides-public/a-40228816

**Die Welt,** Straßenkriminalität: Polizei in NRW setzt häufiger auf Videoüberwachung (DIE WELT, 2021) https://www.welt.de/regionales/nrw/article206038077/Strassenkriminalitaet-Polizei-in-NRW-setzt-haeufiger-auf-Videoueberwachung.html

**Digitalcourage,** 'Perso Ohne Finger' (Digitalcourage 2020) https://aktion.digitalcourage.de/perso-ohne-finger

**Doffman, Z.,** 'New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report' (Forbes, 14 April 2019) www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report

**Do Rzeczy,** 'CBA inwigiluje Polaków przez program Pegasus? Biuro dementuje', (4 Sept 2019) https://ziemkiewicz.dorzeczy.pl/kraj/112878/cba-inwigiluje-polakow-przez-program-pegasus-biuro-dementuje.html

**Dubal, V.,** 'San Francisco was right to ban facial recognition. Surveillance is a real danger' The Guardian (2019): https://www.theguardian.com/commentisfree/2019/may/30/san-francisco-ban-facial-recognition-surveillance

**Ebelt, F.,** 'Union Und SPD Haben Fingerabdruck-Pflicht Beschlossen' (Digitalcourage, 2020) https://digitalcourage.de/blog/2020/fingerabdruck-pflicht%20beschlossen-persoohnefinger

E**uropean Digital Rights,** Ban Biometric Mass Surveillance (Brussels 2020), https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

**European Digital Rights,** 'Facial recognition and fundamental rights 101' Resources (2019): https://edri.org/our-work/facial-recognition-and-fundamental-rights-101

**Edvardsen, S.,** 'How to interpret Sweden's first GDPR fine on facial recognition in school' IAPP (2019) https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school

**Evers, M.,** 'Margatens bedrijf verovert de Arena met gezichtsherkenning' De Limburger (2019) https://www.limburger.nl/cnt/dmf20190515_00105698

**Future Travel Experience,** 'Biometric Technology Enabling Seamless Airport Vision' (Future Travel Experience, 2015) https://www.futuretravelexperience.com/2015/07/biometric-technology-driving-seamless-airport-vision

**Gazeta,** 'Rząd uruchamia aplikację Kwarantanna domowa. 20 minut na wysłanie selfie lub wizyta policji' (20 March 2020) https://next.gazeta.pl/next/7,173953,25806038,rzad-uruchomia-aplikacje-kwarantanna-domowa-20-minut-na-wyslanie.html

**Geiger, G.,** 'How a Discriminatory Algorithm Wrongly Accused Thousands of Families of Fraud' Vice (2021) https://www.vice.com/en/article/jgq35d/how-a-discriminatory-algorithm-wrongly-accused-thousands-of-families-of-fraud

**Gemeente Almere,** Evaluatie pilot digitale deurbel Almere 2018 (Almere 2018) https://veilig.almere.nl/fileadmin/files/almere/beeldbank/veiligheid/Evaluatierapport_digi_deurbel_20190325_def.pdf

**Gemeente Amsterdam,** 'Digitale Parameter' De Digitale Stad https://www.amsterdam.nl/wonen-leefomgeving/innovatie/de-digitale-stad/digitale-perimeter

**Gotink, B.,** 'Slimme camera's herkennen elke carnavalsvierder in Korte Putstraat: 'Wie er niet in mag, hebben we er zo uitgepikt' BD (2019) https://www.bd.nl/den-bosch-vught/slimme-camera-s-herkennen-elke-carnavalsvierder-in-korte-putstraat-wie-er-niet-in-mag-hebben-we-er-zo-uitgepikt~a55f6fdd/?referrer=https%3A%2F%2Fwww.google.com%2F

**Grabowska-Moroz, B.,** 'The Polish surveillance regime before the ECHR' (about:intel, 27 April 2020) https://aboutintel.eu/echr-poland-surveillance

**Guardian staff reporter** "'Living Laboratories': The Dutch Cities Amassing Data on Oblivious Residents." (The Guardian 2018) www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht

**Hao, K.,** 'A US Government Study Confirms Most Face Recognition Systems Are Racist' (MIT Technology Review, 2019) https://www.technologyreview.com/2019/12/20/79/ai-face-recognition-racist-us-government-nist-study

**Hao, K.,** 'This is how AI bias really happens — and why it's so hard to fix' (MIT Technology Review, 2019). https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix

**Heesterbeek, W.,** 'Camera's met gezichtsherkenning bij FC Den Bosch en in het casino: 'Dit kan niet zomaar'' Omroep Brabant (2019) https://www.omroepbrabant.nl/nieuws/3003082/cameras-met-gezichtsherkenning-bij-fc-den-bosch-en-in-het-casino-dit-kan-niet-zomaar

**Heise,** 'G20-Krawalle: Polizei Ignoriert Löschanordnung Des Datenschützers' (Heise, 2021) https://www.heise.de/newsticker/meldung/G20-Krawalle-Polizei-ignoriert-Loeschanordnung-des-Datenschuetzers-4537317.html?wt_mc=rss.ho.beitrag.rss

**Hekkert, P.,** 'Eerste Kamer trapt op de rem bij Super SyRI' FNV (19 January 2021) https://www.fnv.nl/nieuwsbericht/sectornieuws/uitkeringsgerechtigden/2021/01/eerste-kamer-trapt-op-de-rem-bij-super-syri

**Hill, K.,** 'The Secretive Company That Might End Privacy as We Know It' The New York Times (2020) https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

**Hoekstra, D.,** 'Netwerk van hypermoderne camera's op Stratumseind in Eindhoven gaat politie helpen' ED (2017) https://www.ed.nl/eindhoven/netwerk-van-hypermoderne-camera-s-op-stratumseind-in-eindhoven-gaat-politie-helpen~a1e8acee

**Hofmans, T.,** 'Gratis deurbellen tegen criminaliteit: Het twijfelachtige effect en de privacyzorgen' Tweakers (2019) https://tweakers.net/reviews/7524/all/digitale-deurbellen-het-twijfelachtige-effect-en-de-privacyzorgen.html

**Hooyman, P.,** 'Het ware gezicht van gezichtsherkenningstechnologie' Bits of Freedom (Amsterdam 2019). https://www.bitsoffreedom.nl/wp-content/uploads/2019/11/het-ware-gezicht-van-gezichtsherkenningstechnologie.pdf

**Hooyu,** https://www.hooyu.com/h

**Houwing, L.,** 'Hoe de politie haar buitenwettelijke surveillancenetwerk uitbreidt' Bits of Freedom (2020) https://www.bitsoffreedom.nl/2020/02/05/hoe-de-politie-haar-buitenwettelijke-surveillancenetwerk-uitbreidt

**Houwing, L.,** 'In beeld van een buitenwettelijk surveillancenetwerk' Joop (2019) https://joop.bnnvara.nl/opinies/in-beeld-van-een-buitenwettelijk-surveillancenetwerk

**Houwing, L.,** 'Minister komt met zorgwekkende antwoorden op Kamervragen over CATCH' Bits of Freedom (2019) https://www.bitsoffreedom.nl/2019/09/11/minister-komt-met-zorgwekkende-antwoorden-op-kamervragen-over-catch

**Huijbregts, J.,** 'Gouda geeft subsidie voor camera of videodeurbel bij aanmelden politiedatabase' Tweakers (2019) https://tweakers.net/nieuws/160772/gouda-geeft-subsidie-voor-camera-of-videodeurbel-bij-aanmelden-politiedatabase.html

**Huijbregts, J.,** 'Nederlandse politie begint met gezichtsherkenning bij opsporing' Tweakers (2016) https://tweakers.net/nieuws/119105/nederlandse-politie-begint-met-gezichtsherkenning-bij-opsporing.html

**Hulsen, S.,** 'Tienduizenden mensen mogelijk onterecht in gezichtendatabase van de politie' Nu.nl (2021) https://www.nu.nl/tech/6121460/tienduizenden-mensen-mogelijk-onterecht-in-gezichtendatabase-van-de-politie.html

**Interia Biznes,** 'Aplikacja "Kwarantanna domowa" pod lupa. TakeTask odpowiada na watpliwosci branzy i uzytkowników' (21st April 2020) https://biznes.interia.pl/finanse/news-aplikacja-kwarantanna-domowa-pod-lupa-taketask-odpowiada-na-,nId,4445461

**Kameras Stoppen,** 'Klage gegen die Videoüberwachung in Köln' (Kameras Stoppen, 2021) https://kameras-stoppen.org/klage-videobeobachtung-koeln

**Kameras Stoppen,** 'Stand der Videoüberwachungsorte in Köln' (Kameras stoppen, 2020) https://kameras-stoppen.org/videobeobachtung-in-koeln

**Kameras Stoppen,** 'Videoüberwachung Breslauer Platz gestoppt' (Kameras stoppen, 2021) https://kameras-stoppen.org/videoueberwachung-breslauer-platz-gestoppt

**Kamińska, M., Potocka J.,** 'Nowak wpadł przez system Pegasus? Budka żada wyjaśnień ws. inwigilacji opozycji' (RMF24, 23 July 2020) https://www.rmf24.pl/fakty/polska/news-nowak-wpadl-przez-system-pegasus-budka-zada-wyjasnien-ws-inw,nId,4627304

**Kern,** Das Ausweisterminal / Kern – Your technology partner (SmartTerminals) https://www.smart-terminal24.com/de/systeme-software/systeme/ausweisterminal.html

**Kirkpatrick, D.,** 'Israeli software helped Saudis spy on Khashoggi, Lawsuit Says' (NYT, 2nd Dec 2018) https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html

**Korte, A.,** 'Facial-Recognition Technology Cannot Read Emotions, Scientists Say' (American Association for the Advancement of Science, 2020) https://www.aaas.org/news/facial-recognition-technology-cannot-read-emotions-scientists-say

**Kość, W.,** 'Poland's PiS faces questions over Israeli Spyware' (Politico, 6 Sept 2019) https://www.politico.eu/article/poland-pis-israeli-spyware-questions

**Koschyk, M.,** 'Big brother in Berlin: Face recognition technology gets tested' (Deutsche Welle, 31 July 2017) https://www.dw.com/en/big-brother-in-berlin-face-recognition-technology-gets-tested/a-39912905

**Kuitert, G.,** 'Heracles Almelo start proef met gezichstherkenning' Tubantia (2019) https://www.tubantia.nl/heracles/heracles-almelo-start-proef-met-gezichtsherkenning~ad9bd7e6

**Lee, J.,** https://www.biometricupdate.com/201709/ot-morpho-denies-claims-kenyan-biometric-voting-system-was-hacked

**Leurs, T.,** 'Überwachung in Bonn: Polizei nimmt Videokameras am Rheinufer in Betrieb' (General-Anzeiger Bonn 2020). https://ga.de/bonn/stadt-bonn/videoueberwachung-am-rheinufer-bonn-polizei-nimmt-kameras-in-betrieb_aid-53147327

**Lohr, S.,** 'Facial Recognition is Accurate, If You're a White Guy.' (2018) https://www2.cs.duke.edu/courses/spring20/compsci342/netid/readings/facialrecnytimes.pdf

**Mac, R.,** Haskins, C. and McDonald L., 'Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA' Buzzfeed News (2020) https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement

**Marczak, B., Scott-Railton, J., McKune, S., Razzak, B.A., and Deibert, R.,** 'Hide and Seek' (CitizenLab, 18 Sept 2018) pg. 8, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries

**Mobility Networks Logistics,** 'DB-Konzern - Facts & Figures' (Web.archive.org) https://web.archive.org/web/20090426010642/http://www.deutschebahn.com/site/bahn/en/db__group/corporate__group/ata__glance/facts__figures/facts__figures.html

**Money,** '"Kwarantanna domowa" bedzie dzialala rok dluzej. Resort cyfryzacji przedluzyl umowe z twórcami aplikacji' (4th July 2020) https://www.money.pl/gospodarka/kwarantanna-domowa-bedzie-dzialala-rok-dluzej-resort-cyfryzacji-przedluzyl-umowe-z-tworcami-aplikacji-6528240382727809a.html

**Monroy, M.,** Projekt Interoperabilität: EU zahlt 300 Millionen Euro für Erkennung von Gesichtern und Fingerabdrücken. [online] Netzpolitik https://netzpolitik.org/2020/eu-zahlt-300-millionen-euro-fuer-erkennung-von-gesichtern-und-fingerabdruecken

**Muller, F.,** 'Echt of nep? In Zwolle hebben ze identiteitsfraude sneller door' DS (2018) https://www.destentor.nl/zwolle/echt-of-nep-in-zwolle-hebben-ze-identiteitsfraude-sneller-door~ad2273f5/?referrer=https%3A%2F%2Fwww.google.com%2F

**Mur, K.,** 'Careful of privacy violations when installing camera doorbells, privacy watchdog warns' NL Times (2020) https://nltimes.nl/2020/10/06/careful-privacy-violations-installing-camera-doorbells-privacy-watchdog-warns

**Muthuti, R., Monyango F. and Karanja, W.** Strathmore University Centre for Intellectual Property and Information Technology Law 'Investigating Privacy Implications of Biometric Voter Registration in Kenya's 2017 Election Process (2018) https://www.cipit.strathmore.edu/wp-content/uploads/2018/05/Biometrics-Privacy-Report-by-CIPIT.pdf

**Mwere, D.,** 'For credible elections, MPs vote to block Huduma Namba firm' (Nation, 2019) https://nation.africa/kenya/news/for-credible-elections-mps-vote-to-block-huduma-namba-firm-161510

**Neurotechnology,** 'Verifinger Case Study: Polish Biometric Passport System' (2009) https://www.neurotechnology.com/download/CaseStudy_Poland_Biometric_Passport_System.pdf

**NOS Nieuws,** 'Ook in Nederland gezichtsherkenning met omstreden Programma Clearview' NOS (2020) https://nos.nl/artikel/2324950-ook-in-nederland-gezichtsherkenning-met-omstreden-programma-clearview.html

**Noyb,** 'Clearview AI In Der EU Illegal, Aber Nur Begrenze Löschungsanordnung' (noyb, 2021) https://noyb.eu/de/clearview-ai-der-eu-illegal

**NSO Group,** https://www.nsogroup.com

**O'Neill, P.H.,** 'Inside NSO, Israel's billion-dollar spyware giant' (MIT Technology Review, 19 Aug 2020) https://www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights

**Panoptykon Foundation,** 'Aplikacja „Kwarantanna domowa" – obowiązkowe nie oznacza skuteczne' (31 March 2020) https://panoptykon.org/aplikacja-kwarantanna-domowa-obowiazkowa-krytyka

**Panoptykon Foundation,** 'No control over surveillance by Polish intelligence agencies: ECHR demands explanation from the government' (18 Dec 2019) https://en.panoptykon.org/government-surveillance-echr-complaint

**Panoptykon Foundation,** 'Odpowiadamy na pytania o aplikację „Kwarantanna domowa"' (25 March 2020) https://panoptykon.org/aplikacja-kwarantanna-domowa

**Panoptykon Foundation,** 'Poland adopted controversial anti-terrorism law' (22 June 2016) https://en.panoptykon.org/articles/poland-adopted-controversial-anti-terrorism-law

**Platform bescherming burgerrechten,** 'SyRI-coalitie aan Eerste Kamer: 'Super SyRI' blauwdruk voor meer toeslagenaffaires' Nieuws (11 January 2021) https://platformburgerrechten.nl/2021/01/11/syri-coalitie-aan-eerste-kamer-super-syri-blauwdruk-voor-meer-toeslagenaffaires

**Poort, F.,** 'Al 229 duizend bewakingscamera's in Nederland' RTL Nieuws (2019) https://www.rtlnieuws.nl/tech/artikel/4957711/nederland-telt-228530-gemelde-bewakingscameras

**Redactie,** 'Mogelijk tienduizenden Nederlanders onterecht in database voor gezichtsherkenning' de Volkskrant (2021) https://www.volkskrant.nl/nieuws-achtergrond/mogelijk-tienduizenden-nederlanders-onterecht-in-database-voor-gezichtsherkenning~b72d2971

**Redactie,** 'Veel huiseigenaren melden zich aan voor Camera in Beeld' Beveiligingsnieuws (2019) https://beveiligingnieuws.nl/nieuws/veel-huiseigenaren-melden-zich-aan-voor-camera-in-beeld

**Rhue, L.,** Racial Influence on Automated Perceptions of Emotions (November 9, 2018). https://ssrn.com/abstract=3281765 or http://dx.doi.org/10.2139/ssrn.3281765

**RTL Nieuws,** 'Gezichtsherkenning in de openbare ruimte: moeten we daar blij mee zijn?' RTL (2020) https://www.rtlnieuws.nl/nieuws/nederland/artikel/4997021/gezichtsherkenning-openbare-ruimte-bits-freedom-digitaal-online

**RP Online,** 'Hier gibt es Videoüberwachung in Mönchengladbach' (RP Online) available at https://rp-online.de/nrw/staedte/moenchengladbach/hier-gibt-es-videoueberwachung-in-moenchengladbach_bid-9124669

**Rychlewska, A.,** 'O PRZEPISIE ART. 168A K.P.K. JAKO PRZYZWOLENIU NA KORZYSTANIE W RAMACH PROCESU KARNEGO Z DOWODÓW ZDOBYTYCH W SPOSÓB NIELEGALNY' (Palestra, May 2016) https://palestra.pl/pl/czasopismo/wydanie/5-2016/artykul/o-przepisie-art.-168a-k.p.k.-jako-przyzwoleniu-na-korzystanie-w-ramach-procesu-karnego-z-dowodow-zdobytych-w-sposob-nielegalny

**Schiphol,** 'Schiphol launches pilot for boarding by means of facial recognition' Schiphol News (2019) https://news.schiphol.com/schiphol-launches-pilot-for-boarding-by-means-of-facial-recognition

**Scott, M. and Wanat, Z.** 'Poland's coronavirus app offers playbook for other governments' (Politico, 2 April 2020) https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments

**Security Management,** 'Stratumseind Eindhoven: hoger veiligheidsgevoel én leuker door Living Lab' Achtergrond (2018) https://www.securitymanagement.nl/stratumseind-eindhoven-living-lab/?vakmedianet-approve-cookies=1&_ga=2.157495482.1453296129.1606072868-157017026.1606072868

**Siedentop, C.,** 'Nach Gewalttat in Mönchengladbach: Bessere Videoüberwachung soll Bürger schützen' (RP ONLINE 2012) https://rp-online.de/nrw/panorama/bessere-videoueberwachung-soll-buerger-schuetzen_aid-13675387

**Signs,** 'Twórcy aplikacji „Kwarantanna domowa" odpowiadaja na zarzuty' (17th April 2020) https://www.signs.pl/tworcy-aplikacji-_kwarantanna-domowa_-odpowiadaja-na-zarzuty,386627,artykul.html

**Simonite, T**. 'Photo Algorithms ID White Men Fine—Black Women, Not So Much' Wired (2018) https://www.wired.com/story/photo-algorithms-id-white-men-fineblack-women-not-so-much

**Srivastava, M. and Wilson, T.,** 'Inside the WhatsApp hack: how an Israeli technology was used to spy' (Financial Times, 30 Oct 2019) https://www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229

**Statline,** 'Geregistreerde criminaliteit; soort misdrijf, regio' Opendata CBS (2021) https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?fromstatweb

**Stoker, E.,** 'CSI in de polder: politie zoekt verdachten met gezichsherkenning' de Volkskrant (2016) https://www.volkskrant.nl/nieuws-achtergrond/csi-in-de-polder-politie-zoekt-verdachten-met-gezichtsherkenning~bde94cf6

**Studio Alphen,** 'Autoriteit Persoonsgegevens onderzoekt gezichtsherkenning bij supermarkt Jumbo' Studio Alphen Nieuws https://www.studioalphen.nl/nieuws/autoriteit-persoonsgegevens-onderzoekt-gezichtsherkenning-bij-supermarkt-jumbo

**TechTrendsKE,** 'French firm OT-Morpho says IEBC voting system was not hijacked' https://techtrendske.co.ke/french-firm-ot-morpho-says-iebc

**The Hague Security Delta,** 'Stratumseind' Living Labs for Security Innovations (2020) https://www.thehaguesecuritydelta.com/innovation/living-labs/lab/3-stratumseind

**Kist, R.,** 'Politiesoftware scant gezichten van verdachten' NRC (2018) https://www.nrc.nl/nieuws/2018/02/19/politiesoftware-scant-gezichten-van-verdachten-a1592781#:~:text=De%20software%2C%20genaamd%20'CATCH',identiteit%20van%20een%20misdadiger%20op

**Telepolis,** 'Kwarantanna domowa będzie działać dłużej, dodatkowo w języku rosyjskim i ukraińskim' (7th July 2020) https://www.telepolis.pl/wiadomosci/aplikacje/kwarantanna-domowa-rok-dluzej-rosyjski-ukrainski

**TVN24,** 'Czarno na białym: Oprogramowanie Pegasus' (28 Aug 2019), available at https://tvn24.pl/go/programy,7/czarno-na-bialym-odcinki,11367/odcinek-50,S00E50,95066

**TVN24,** 'Czy CBA ma narzędzie totalnej inwigilacji? "Infrastruktura systemu powiązana z Polską"' (29 Aug 2019) https://tvn24.pl/polska/system-pegasus-i-pytania-do-cba-czarno-na-bialym-ra964972-2312092

**TVN24,** 'Komendant Główny Policji: prawdopodobnie 600 przypadków niestosowania się do kwarantanny' (19 March 2020) https://tvn24.pl/najnowsze/koronawirus-w-polsce-komendant-glowny-policji-600-przypadkow-niestosowania-sie-do-kwarantanny-4368858

**Twente, R.,** 'Nieuw communicatienetwerk Tec4se ondersteunt veiligheids- en hulpverleningsdiensten bij inzet' Nieuws (2014) https://www.regiotwente.nl/over-regio-twente/pers-en-media/nieuws/731-nieuw-communicatienetwerk-tec4se-ondersteunt-veiligheids-en-hulpverleningsdiensten-bij-inzet

**Uibu, K.,** 'Poland is making its citizens use a 'selfie' app during the coronavirus crisis' (ABC, 24 April 2020) https://www.abc.net.au/news/2020-04-25/coronavirus-poland-tracking-quarantine-selfie-app/12173884

**Videmo,** Videmo 360' (Videmo) https://videmo.de/en/products/videmo-360

**VISA,** 'Goodbye, Passwords. Hello, Biometrics' (2017) https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-biometrics-payments-study.pdf

**Vodafone Institute for Society and Communications,** https://www.vodafone-institut.de/bigdata/links/VodafoneInstitute-Survey-BigData-Highlights-en.pdf

**Van Dijk, M.,** 'Stratumseind: Eindhoven's Data Street' Innovation Origins (2018) https://innovationorigins.com/stratumseind-eindhovens-data-street

**Van Gaal, W.,** 'Gezichtsherkenning op de Nederlandse straten: moeten we dat willen?' VICE (2019) https://www.vice.com/nl/article/8xzydz/gezichtsherkenning-op-de-nederlandse-straten-moeten-we-dat-willen

**Van Helvert, M.,** 'Tientallen camera's houden klanten van filiaal Jumbo in the gaten: 'Willen we dit?'' RTL Nieuws (2019) https://www.rtlnieuws.nl/nieuws/nederland/artikel/4941596/gezichtsherkenning-biometrie-alphen-jumbo-privacy

**Van Monsjou, D.,** 'Bijna 9 op de 10 geregistreerde beveiligingscamera's filmen openbare weg' Tweakers (2019) https://tweakers.net/nieuws/161164/bijna-9-op-de-10-geregistreerde-beveiligingscameras-filmen-openbare-weg.html

**Waarlo, N. and Verhagen, L.,** 'De stand van gezichtsherkenning in Nederland' de Volkskrant (2020) https://www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028

**Whittaker, Z.,** 'AdultFriendFinder Network Hack Exposes 412 Million Accounts' (ZDNet, 13 November 2016) www.zdnet.com/article/adultfriendfinder-network-hack-exposes-secrets-of-412-million-users

**Winter, B.,** 'RET voegt gezichtsherkenning toe aan camerabewaking' Nu.nl (2011) https://www.nu.nl/binnenland/2613144/ret-voegt-gezichtsherkenning-toe-camerabewaking.html

**Wprost,** 'Sprawa Nowaka pretekstem do inwigilacji sztabu Trzaskowskiego? Kamiński odpowiada na tezy Budki' (23 July 2020) https://www.wprost.pl/kraj/10346788/sprawa-nowaka-pretekstem-do-inwigilacji-sztabu-trzaskowskiego-kaminski-odpowiada-na-tezy-budki.html

**Wprost,** 'Za aplikacje „Kwarantanna domowa" odpowiada polska spółka TakeTask. Inne kraje też zainteresowane' (7 April 2020) https://biznes.wprost.pl/technologie/10313034/za-aplikacje-kwarantanna-domowa-odpowiada-polska-spolka-taketask-inne-kraje-tez-zainteresowane.html

**Yang, Y., and Murgia, M.,** 'Facial recognition: how China cornered the surveillance market' Financial Times (2019) https://www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385

### Government Publications

**Alessandra Pierucci & Jean-Philippe Walter,** 'Joint Statement on Digital Contact Tracing' (Council of Europe Committee of Convention 108, 28 April 2020)

**Autoriteit Persoonsgegevens,** 'Basisregistratie Personen (BRP)' Overheid (2021) available at: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/overheid/basisregistratie-personen-brp

**Autoriteit Persoonsgegevens,** 'Biometrie' Identificatie (2021) available at: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/biometrie#faq

**Autoriteit Persoonsgegevens,** 'Cameratoezicht op openbare plaatsen' Foto en Film (2021) available at: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/foto-en-film/cameratoezicht-op-openbare-plaatsen#onder-welke-voorwaarden-mag-een-gemeente-cameratoezicht-inzetten-7758

**Autoriteit Persoonsgegevens,** 'Formele Waarschuwing AP aan supermarket om gezichtsherkenning' AP Nieuws (15 December 2020) available at: https://autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning

**Autoriteit Persoonsgegevens,** 'Waarborg privacy in de ontwikkeling van Smart Cities' Nieuws (2019) available at: https://autoriteitpersoonsgegevens.nl/nl/nieuws/waarborg-privacy-de-ontwikkeling-van-smart-cities

**Brainport Eindhoven,** 'Kunstmatige intelligentie ondersteunt Stadstoezicht en politie tijdens carnaval' Link Magazine (2020) available at: https://www.linkmagazine.nl/kunstmatige-intelligentie-ondersteunt-stadstoezicht-en-politie-tijdens-carnaval

**Bundesministerium des Innern, für Bau und Heimat,** 'Bundesregierung Und Deutsche Bahn Beschließen Weitere Maßnahmen Für Mehr Sicherheit An Bahnhöfen' (2020) https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/sicherheit-bahnhoefe.html

**Bundesdruckerei,** ePASS Fibel (2007) available at https://web.archive.org/web/20101031204925/http://bundesdruckerei.de/de/produkte/produkte_dokument/dok_persausw/download/produkte_sicherheit.pdf

**Centre for Strategy and Evaluation Services,** 'Study to Support the Preparation of an Impact Assessment on EU Policy Initiatives on Residence and Identity Documents to Facilitate the Exercise of the Right of Free Movement' (28 Aug 2017)

**Council of Europe,** 'Joint Statement on the right to data protection in the context of the COVID-19 pandemic (30 March 2020) https://rm.coe.int/covid19-joint-statement/16809e09f4

**'Dane biometryczne mogą być wykorzystywane tylko w wyjątkowych sytuacjach'** (UODO, 3rd March 2021) https://uodo.gov.pl/pl/138/1943

**Deutscher Bundestag,** 2020. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Torsten Herbst, Frank Sitta, Oliver Luksic, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/16870 – Sicherheit in Zügen und an Bahnhöfen avaialble at https://dip21.bundestag.de/dip21/btd/19/174/1917436.pdf

**Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit** ('HmbBfDI'), 'Pressemitteilung: Einführung der automatisierten Gesichtserkennung beanstandet' (2018) Available at: https://datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360

**European Commission,** Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178

**HmbBfDI,** ' Anfrage #195578: Fragenkatalog An Clearview AI' (2020) available at https://fragdenstaat.de/anfrage/fragenkatalog-an-clearview

**HmbBfDI,** 'Antrag auf Zulassung der Berufung §§ 124, 124a VwGO Az. 5 Bf 46/20.Z - Begründung des Antrags vom 6.2.2020' (to Hamburg Administrative Appeal Court 2020) available at https://datenschutz-hamburg.de/assets/pdf/Antrag_Zulassung_Berufung_2020-03-13.pdf

**HmbBfDI,** 'Az.: 11.03-13 - Einsatz Der Gesichtserkennungssoftware „Videmo 360" Durch Die Polizei Hamburg Zur Aufklärung Von Straftaten Im Zusammenhang Mit Dem In Hamburg Stattgefundenen G20- Gipfel' (2021) available at https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

**HmbBfDI,** 'Consultation Prior To An Order Pursuant To Article 58(2)(G) GDPR' (2021) available at https://noyb.eu/sites/default/files/2021-01/545_2020_Anh%C3%B6rung_CVAI_ENG_Redacted.pdf

**HmbBfDI**, Einsatz der Gesichtserkennungssoftware „Videmo 360" durch die Polizei Hamburg zur Aufklärung von Straftaten im Zusammenhang mit dem in Hamburg stattgefundenen G20- Gipfel. (Hamburg, 2018). Available at: https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

**HmbBfDI,** 'Polizei Hamburg Löscht Die Im Zuge Der G20-Ermittlungen Erstellte Biometrische Datenbank Zum Gesichtsabgleich' (2020) available at https://datenschutz-hamburg.de/pressemitteilungen/2020/05/2020-05-28-datenbank-loeschung ('HmbBfDI Press Release 2020')

**HmbBfDI,** 'Stellungnahme Des Hmbbfdi Vom 20. Juli 2020 Zur Zulässigkeit Der Berufung Az.: J / 11.03-13' (2020) available at https://datenschutz-hamburg.de/assets/pdf/Stellungnahme_Zulassung_Berufung_2020-07-20.pdf

**Ministry of Digitalisation,** 'Dowód osobisty — informacja o dokumencie' (6 March 2019) https://obywatel.gov.pl/pl/dokumenty-i-dane-osobowe/dowod-osobisty-informacja-o-dokumencie

**'Namensänderung'** (Nuernberg.de) https://www.nuernberg.de/internet/ordnungsamt/namensaenderung.html

**NIK,** "Assistance to crime victims as part of the Victims' Aid Fund"(2016-2017) https://www.nik.gov.pl/plik/id,17115,vp,19675.pdf

**Ombudsman,** 'Apel RPO do Prezydenta w sprawie ustawy antyterrorystycznej' (21 June 2016) https://www.rpo.gov.pl/pl/content/apel-rpo-do-prezydenta-w-sprawie-ustawy-antyterrorystycznej

**Platform bescherming burgerrechten,** 'SyRI-coalitie aan Eerste Kamer: 'Super SyRI' blauwdruk voor meer toeslagenaffaires' Nieuws (11 January 2021) available at: https://platformburgerrechten.nl/2021/01/11/syri-coalitie-aan-eerste-kamer-super-syri-blauwdruk-voor-meer-toeslagenaffaires

**Polish Government,** 'Aplikacja Kwarantanna domowa – od dziś obowiazkowa' (1 April 2020) https://www.gov.pl/web/koronawirus/aplikacja-kwarantanna-domowa--od-dzis-obowiazkowa

**Polish Government,** 'Ponad 10 tysięcy osób korzysta z naszej aplikacji Kwarantanna Domowa! Odpowiadamy na Wasze pytania' (23rd March 2020) https://www.gov.pl/web/cyfryzacja/ponad-10-tysiecy-osob-korzysta-z-naszej-aplikacji-kwarantanna-domowa-odpowiadamy-na-wasze-pytania#:~:text=Ch%C4%99tnie%20na%20wszystkie%20odpowie-my!,pe%C5%82nego%20korzystania%20z%20naszej%20apki

**Politie Nederland,** 'Camera in Beeld' Thema's (2020) available at: https://www.politie.nl/themas/camera-in-beeld.html?sid=07c1d5df-60bf-470a-993f-f9f212c9dd00

**Politie Nederland,** 'Tweehonderdduizend extra 'ogen' voor politie' Nieuws (2019) available at: https://www.politie.nl/nieuws/2019/januari/10/tweehonderdduizend-extra-%E2%80%98ogen%E2%80%99-voor-politie.html

**Security Management,** 'Stratumseind Eindhoven: hoger veiligheidsgevoel én leuker door Living Lab' Achtergrond (2018) available at: https://www.securitymanagement.nl/stratumseind-eindhoven-living-lab/?vakmedianet-approve-cookies=1&_ga=2.157495482.1453296129.1606072868-157017026.1606072868

**'Sicherheitsbahnhof Berlin Südkreuz'** (Bundesministerium des Innern, für Bau und Heimat 2017) https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html

**Stadt Ludwigsburg,** 'Anfrage #205072: Abholautomat für Ausweise' (5 December 2020) available at: https://fragdenstaat.de/anfrage/abholautomat-fur-ausweise-1

**Stadt Langenhagen,** 'Anfrage #205071: Einwilligungserklrung Abholstation und Datenschutzinformation' (14 December 2020) available at: https://fragdenstaat.de/anfrage/abholautomat-fur-ausweise

**Verwaltungsgericht Köln,** (18 January 2021) Az.: 20 L 2340/19, available at http://www.justiz.nrw.de/nrwe/ovgs/vg_koeln/j2021/20_L_2340_19_Beschluss_20210118.html ('20 L 2340/19')

**"The Dutch GDPR Implementation Act and the Use of Biometric Data"** (2020) https://www.akd.eu/insights/the-dutch-gdpr-implementation-act-and-the-use-of-biometric-data

**The Hague Security Delta,** 'Stratumseind' Living Labs for Security Innovations (2020) available at: https://www.thehaguesecuritydelta.com/innovation/living-labs/lab/3-stratumseind

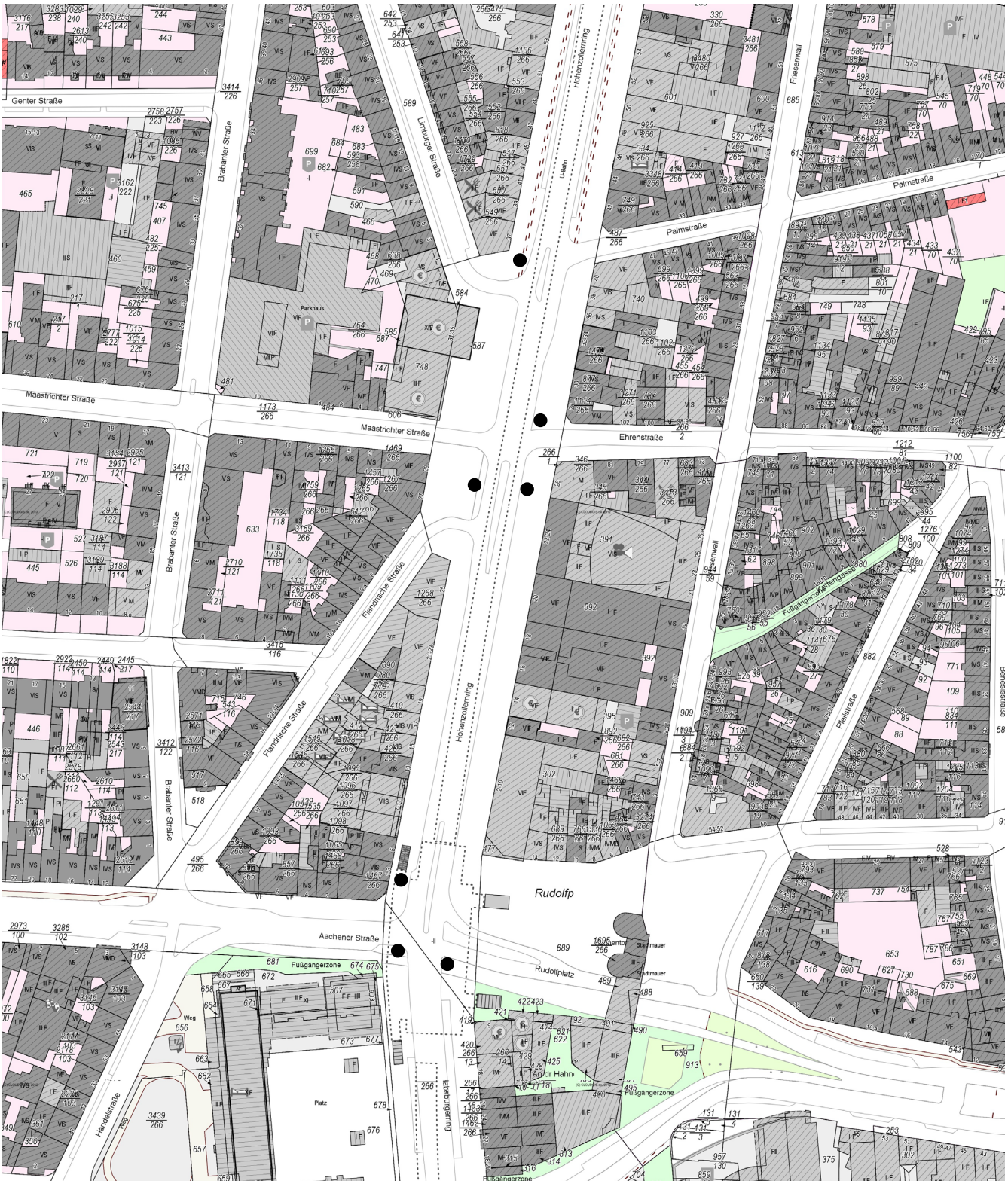
**Tweede Kamer der Staten-Generaal,** Kamerstuk 32761 nr. 152: Verwerking en bescherming persoonsgegevens - Brief van de Minister van Justitie en Veiligheid (25th of November 2019), available at: https://zoek.officielebekendmakingen.nl/kst-32761-152.html

**UK Government,** 'New legal duty to self isolate comes into force today' (28 Sept 2020) https://www.gov.uk/government/news/new-legal-duty-to-self-isolate-comes-into-force-today

# ANNEX 1


**Source: Cologne Police,**
'Videoüberwachung Breslauer Platz'
available at https://koeln.polizei.nrw/sites/default/files/2018-04/Kamerapositionen-Videobeobachtung-Breslauer-Platz.jpg

# ANNEX 2




**Source: Cologne Police,** available at https://koeln.polizei.nrw/sites/default/files/2017-12/k-standorte-kameras-ringe1_0.pdf

# Mass surveillance. Random Censorship. Content Restrictions.

Companies and governments increasingly restrict our freedoms.

–

DONATE NOW:

https://edri.org/take-action/donate

**Press enquiries**
press@edri.org

**Brussels office**
brussels@edri.org

**Phone number**
+32 2 274 25 70

**Visit us**
Rue Belliard 12
1040 Brussels
Belgium

**Follow us**
Twitter
Facebook
LinkedIn
Youtube



EDRi

EUROPEAN DIGITAL RIGHTS

**European Digital Rights (EDRi)** is the biggest European network defending rights and freedoms online. We promote, protect and uphold human rights and the rule of law in the digital environment, including the right to privacy, data protection, freedom of expression and information.

**www.edri.org**