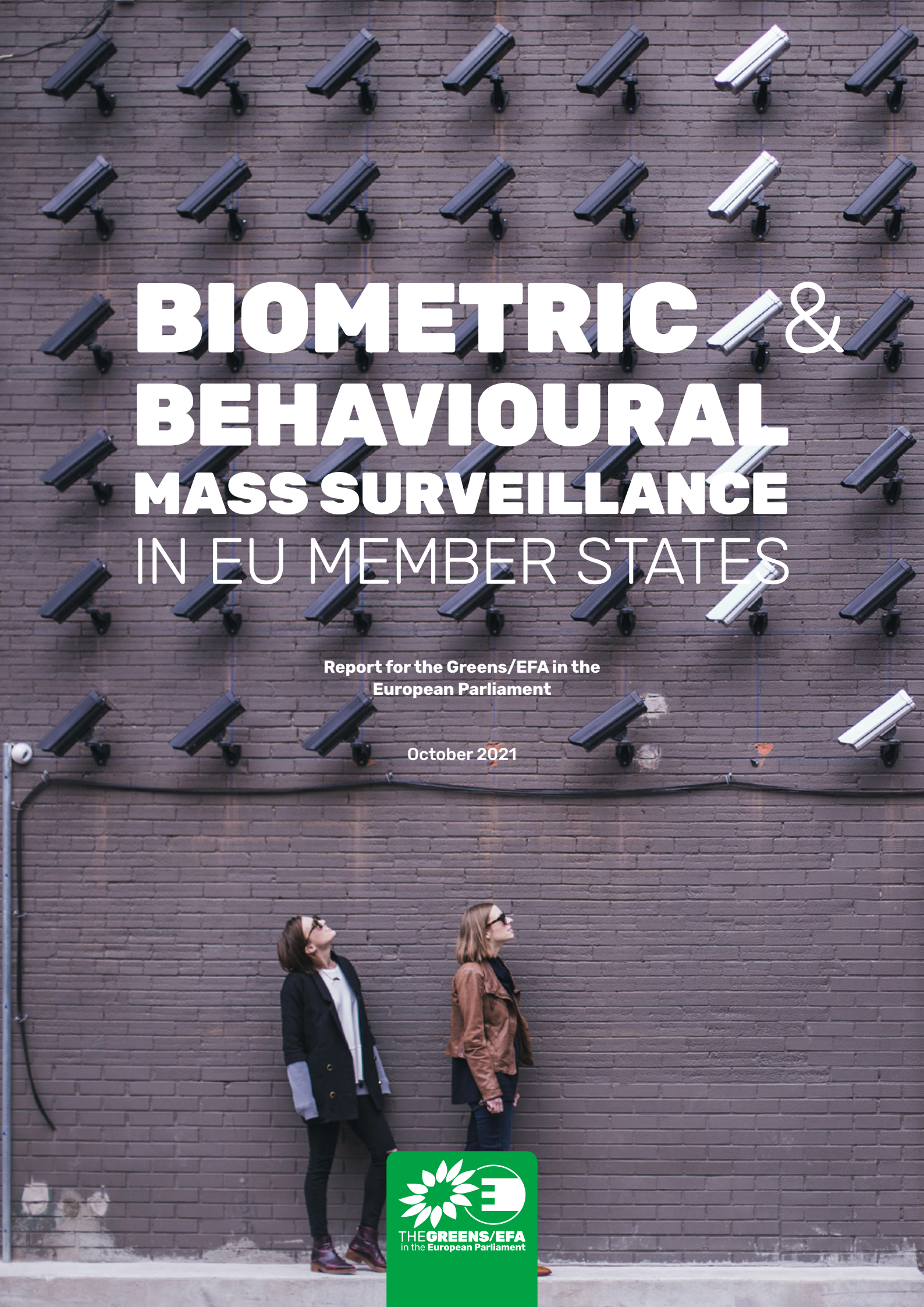
Biometric and behavioural mass surveillance in EU member states: report for the Greens/EFA in the European Parliament

Ragazzi, F.P.S.M.; Kuskonmaz, E.; Plájás, I.; Ven, R.R. van de; Wagner, B.

Citation
Ragazzi, F. P. S. M., Kuskonmaz, E., Plájás, I., Ven, R. R. van de, & Wagner, B. (2021). *Biometric and behavioural mass surveillance in EU member states: report for the Greens/EFA in the European Parliament*. Brussels: Greens/EFA. Retrieved from https://hdl.handle.net/1887/3256585

Version:	Not Applicable (or Unknown)
License:	Leiden University Non-exclusive license
Downloaded from:	https://hdl.handle.net/1887/3256585

Note: To cite this publication please use the final published version (if applicable).



BIOMETRIC & BEHAVIOURAL MASS SURVEILLANCE IN EU MEMBER STATES

Report for the Greens/EFA in the European Parliament

October 2021

THE GREENS/EFA in the European Parliament

TABLE OF CONTENTS

4 **AUTHORS**

5 **ACRONYMS**

7 **EXECUTIVE SUMMARY**

15 **CHAPTER 1. Introduction**
16 1.1 Objectives of the report
17 1.2 The international context
18 1.3 The European context
19 1.4 Four positions in the policy debates
20 1.5 Lack of transparency and the stifling of public debate
21 1.6 Scope and working definitions
22 1.7 Methodology

23 **PART I: OVERVIEW OF EUROPEAN PRACTICES**

25 **CHAPTER 2. Technical overview**
26 2.1 Remote Biometric Identification and classification: defining key terms
26 2.2 Detection vs recognition
26 2.3 Facial Recognition: verification/authentication vs identification
27 2.4 Forensic (ex-post) vs Live Facial Recognition
27 2.5 Other systems: gait recognition, emotion recognition
28 2.6 How does image-based remote biometric identification work?
31 2.7 Technical limits, problems, and challenges of facial recognition

36 **CHAPTER 3. Overview of deployments in Europe**
37 3.1 Authentication
41 3.2 Surveillance
44 3.3 Remote Biometric Identification
45 3.4 Conclusion

47 **CHAPTER 4. Legal bases**
48 4.1 EU Fundamental Rights Framework for the Right to Privacy and the Right to Protection o Personal Data
50 4.2 EU Secondary Law: GDPR & LED
53 4.3 EU Soft law: Convention 108+

55 **CHAPTER 5. Main political issues and debates**
57 5.1 The emergence of remote biometric identification as a policy issue
57 5.2 Four positions in the policy debates
62 5.3 EU Commission Proposal on the Regulation for the Artificial Intelligence Act

TABLE OF CONTENTS

65 **PART II: CASE STUDIES**

67 **CHAPTER 6. Facial Recognition cameras at Brussels International Airport (Belgium)**
68 6.1 The Zaventem pilot in the context of Face Recognition Technology in Belgium
69 6.2 Legal bases and challenges
71 6.3 Mobilisations and contestations
72 6.4 Effects of the technologies

74 **CHAPTER 7. The Burglary Free Neighbourhood in Rotterdam (Netherlands)**
75 7.1 Detection and decision-making in the "Burglary free neighbourhood" Fieldlab
77 7.2 Legal bases and challenges
78 7.3 Mobilisations and contestations
79 7.4 Effects of the technologies

83 **CHAPTER 8. The Safe City Projects in Nice (France)**
84 8.1 The various facets of the "Safe city" project in Nice
85 8.2 Legal bases and challenges
86 8.3 Mobilisations and contestations
88 8.4 Effects of the technologies

90 **CHAPTER 9. Facial Recognition in Hamburg, Mannheim & Berlin (Germany)**
91 9.1 RBI Deployments in Germany
92 9.2 Legal bases and challenges
95 9.3 Mobilisations and contestations
96 9.4 Effects of the technologies: normalising surveillance

98 **CHAPTER 10. The Dragonfly project (Hungary)**
99 10.1 Remote Biometric Identification in Hungary
102 10.2 Legal bases and challenges
103 10.3 Mobilisations and contestations
105 10.4 Effects of the technologies

107 **CHAPTER 11. Recommendations**

110 **REFERENCES**

118 **ANNEX: CASES**
118 11.1 CJEU Decisions
118 11.2 ECtHR decisions
118 11.3 Decisions of National Courts

AUTHORS

Dr. Francesco Ragazzi (scientific coordinator) is an associate professor in International Relations at Leiden University (Netherlands), an associated scholar at the Centre d'Etude sur les Conflits, Liberté et Sécurité (France). He holds a PhD in Political Science from Sciences Po Paris (France) and Northwestern University (USA). His research interests include radicalisation, terrorism, and mass surveillance. His current research project, Security Vision, funded by a European Research Council Consolidator Grant analyses the politics of computer vision in the field of security. His work has been published in numerous peer-reviewed journals and edited volumes. He serves on the editorial board of the journals International Political Sociology, Citizenship Studies and Cultures & Conflits. He has been consulted as an expert on issues of security by the European Parliament, for whom he has co-authored several reports, the Council of Europe and the French Senate.

Dr. Elif Mendos Kuskonmaz is a lecturer at the School of Law at the University of Portsmouth. She holds a Master's Degree in Public Law from Istanbul University, and an LLM in Public International Law and a PhD from Queen Mary University of London. She researches on surveillance measures and the nexus with the right to privacy and data protection. Elif is also a registered lawyer with the Istanbul Bar Association.

Ildikó Z Plájás is a post-doctoral researcher at the Institute of Political Science, Leiden University. She has studied anthropology and cultural studies in Romania and Hungary, later graduating in Visual Ethnography at Leiden University, the Netherlands. She is currently completing her PhD at the University of Amsterdam. Her research examines how visual technologies in governance enact certain groups of people as "racial others" in Europe.

Ruben van de Ven is a PhD candidate in Political Science at the Institute of Political Science, Leiden University. His PhD project studies the ethical and political implications of surveillance algorithms that order human gestures. Since graduating from the Master in Media Design programme at the Piet Zwart Institute, he has researched algorithmic politics through media art, computer programming and scholarly work. He has focused on how the human individual becomes both the subject of and input into machine learning processes. Earlier artistic work on the quantification of emotions examined the transformation of humanistic concepts as they are digitised. His work has been presented at both art exhibitions and academic conferences.

Dr Ben Wagner is an assistant professor at the Faculty of Technology, Policy and Management at TU Delft, where his research focuses on technology policy, human rights and accountable information systems. He is Associate Faculty at the Complexity Science Hub Vienna and a visiting researcher at the Human Centred Computing Group, University of Oxford. He previously worked at WU Vienna, TU-Berlin, the University of Pennsylvania and European University Viadrina. He holds a PhD in Political and Social Sciences from the European University Institute in Florence

ACRONYMS

ABIS	Automated Biometric Identification Systems
ACLU	American Civil Liberties Union
ADM	Automated Decision-Making (System)
AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligence
ANPR	Automated Number Plate Recognition
API	Application Programming Interface
AWS	Amazon Web Services
BDAS	Biometric Data Processing System
BDSG	Federal Data Protection Act (Germany)
BKA	Federal Criminal Police Office (Germany)
BKK	Centre for Budapest Transport (Hungary)
BPI	Public Investment Bank (France)
BPOL	German Federal Police
CATCH	Central Automatic TeChnology for Recognition of Persons (Netherlands)
CBIS	Central Biometric Information System (Czechia)
CCTV	Closed Circuit Television
CGT	General Labour Confederation (France)
CJEU	Court of Justice of the European Union (EU)
CNIL	National Commission for Informatics and Freedoms (France)
COC	Supervisory Body for Police Information (Belgium)
CoE	Council of Europe
COCO	Common Objects in Context (Dataset)
COVID	Coronavirus Disease
CSU	Centre for Urban Supervision (France)
DEP	Digital European Program
DITSS	Dutch Institute for Technology, Safety & Security
DPA	Data Protection Authority
EC	European Commission (EU)
ECtHR	European Court of Human Rights
EDE	Criminal identification database (Austria)
EDPB	European Data Protection Board (EU)
EDPS	European Data Protection Supervisor (EU)
EDS	European Data Strategy
EEA	European Economic Area
EPP	European People's Party
EU	European Union
FRA	Fundamental Rights Agency (EU)
FRT	Facial Recognition Technology
FRVT	Face Recognition Vendor Test
GDPR	General Data Protection Regulation (EU)
HCLU	Hungarian Civil Liberties Union (Hungary). See "
HD	High Definition
HDR	Habitoscopic Data Register
HKR	Home Quarantine App (Hungary)
IARPA	Intelligence Advanced Research Projects Agency (USA)
ID	Identification
IFRS	Interpol Facial R
IKSZR	Integrated Traffic Management and Control System (Hungary)
INCLO	International Network of Civil Liberties Organisations
INPOL	Criminal Case Management System (Germany)
KAK	Governmental Data Centre (Hungary)

ACRONYMS

KDNP	Christian Democratic People's Party (Hungary)
LED	Law Enforcement Directive (EU)
LFP	Law on the Function of Police (Belgium)
LGBTQ	Lesbian, Gay, Bisexual,Transgender, Queer
LIDAR	Light Detection and Ranging
LPA	Airport Police (Belgium)
LQDN	La Quadrature du Net (France)
GMO	Genetically Modified Organism
MIT	Massachusetts Institute of Technology
MRAP	Movement against racism and for friendship between peoples (France)
NAIH	Hungarian National Authority for Data Protection and Freedom of Information
NBIS	National Biometric Identification System (Romania)
NGO	Non-Governmental Organisation
NIST	National Institute of Standards and Technology (USA)
NISZ	National Infocommunication Services (Hungary)
PARAFE	Rapid passage at the external borders (France)
PPM	Pixels Per Meter
RBI	Remote Biometric Identification
RETU	Registered persons identifying features database and Aliens database (Finland)
RGB	Red, Green, Blue
SIS	Schengen Information System
SSNS	Secret Service for National Security (Hungary)
TAJ	Criminal case history database (France)
TASZ	Hungarian Civil Liberties Union
TELEFI	Towards the European Level Exchange of Facial Images (EU Project)
UAVG	GDPR Implementation Act (Germany)
UK	United Kingdom
UN	United Nations
UNHRC	United Nations Human Rights Council
US(A)	United States of America
VGG	Visual Geometry Group (Dataset)
VMD	Video motion detection
VOC	Visual Object Classes (Pascal VOC)
YOLO	You Only Look Once (Algorithm)

EXECUTIVE SUMMARY

CHAPTER 1: INTRODUCTION

The aim of this report is to establish a problematised overview of what we know about what is currently being done in Europe when it comes to remote biometric identification (RBI), and to assess in which cases we could potentially fall into forms of biometric mass surveillance.

Private and public actors are increasingly deploying "smart surveillance" solutions including RBI technologies which, if left unchecked, could become biometric mass surveillance. Facial recognition technology has been the most discussed of the RBI technologies. However, there seems to be little understanding of the ways in which this technology might be applied and the potential impact of such a broad range of applications on the fundamental rights of European citizens.

The development of RBI systems by authoritarian regimes which may subsequently be exported to and used within Europe is of concern. Not only as it pertains to the deployments of such technologies but also the lack of adequate insight into the privacy practices of the companies supplying the systems.
Four main positions have emerged among political actors with regard to the deployments of RBI technologies and their potential impact on fundamental rights: 1) active promotion 2) support with safeguards; 3) moratorium and 4) outright ban.

CHAPTER 2: TECHNICAL OVERVIEW

The current market of RBI systems is overwhelmingly dominated by image-based products, at the centre of which is facial recognition technology (FRT). Other products such as face detection and person detection technologies are also in use.
FRT is typically being deployed to perform two types of searches: cooperative searches for verification and/ or authentication purposes, and non-cooperative searches to identify a data subject. The former involves voluntary consent from the data subject to capture their image, while the latter may not.
Live facial recognition is currently the most controversial deployment of FRT: Live video feeds are used to generate snapshots of individuals and then match them against a database of known individuals – the "watchlist".
Other RBI technologies are being deployed though their use at present is marginal compared to FRT, these include gait (movement), audio, and emotion recognition technologies, amongst others.

A better understanding of the technical components and possible usage applications of

image-based RBI technologies is needed in order to assess their potential political implications.
RBI technologies are subject to technical challenges and limitations which should be considered in any broader analysis of their ethical, legal, and political implications.

CHAPTER 3: OVERVIEW OF DEPLOYMENTS IN EUROPE

Current deployments of RBI technologies within Europe are primarily experimental and localised. However, the technology coexists with a broad range of algorithmic processing of security images being carried out on a scale which ranges from the individual level to what could be classed as biometric mass surveillance. Distinguishing the various characteristics of these deployments is not only important to inform the public debate, but also helps to focus the discussion on the most problematic uses of the technologies.

Image and sound-based security applications being used for authentication purposes do not currently pose a risk for biometric mass surveillance. However, it should be noted that an alteration to the legal framework could increase the risk of them being deployed for biometric mass surveillance especially as many of the databases being used contain millions of data subjects.
In addition to authentication, image and sound-based security applications are being deployed for surveillance. Surveillance applications include the deployment of RBI in public spaces.

Progress on two fronts makes the development of biometric mass surveillance more than a remote possibility. Firstly, the current creation and/or upgrading of biometric databases being used in civil and criminal registries. Secondly, the repeated piloting of live-feed systems connected to remote facial and biometric information search and recognition algorithms.

CHAPTER 4: LEGAL BASES

The use of biometric tools for law enforcement purposes in public spaces raises a key issue of the legal permissibility in relation to the collection, retention and processing of data when considering the individual's fundamental rights to privacy and personal data protection. When viewed through this lens, RBI technologies could have a grave impact on the exercise of a range of fundamental rights.

The deployment of biometric surveillance in public spaces must be subject to strict scrutiny in order to avoid circumstances which could lead to mass surveillance. This includes targeted surveillance which has the potential for indiscriminate collection of data on any persons present in the surveilled location, not only that of the target data subject.
The normative legal framework for conducting biometric surveillance in public spaces can be found in the EU secondary legislation on data protection (GDPR and LED). The use of biometric data under this framework must be reviewed in light of the protection offered by fundamental rights.

The European Commission's April 2021 proposal on the Regulation for the Artificial Intelligence Act aims to harmonise regulatory rules for Member States on AI-based systems. The Proposed Regulation lays out rules focused on three categories of risks (unacceptable, high, and low/ minimal risk) and anticipates covering the use of RBI systems. It also aims to compliment the rules and obligations set out in the GDPR and LED.

CHAPTER 5: POLITICAL DEVELOPMENTS AND MAIN ISSUES OF CONTENTION

Four main positions on RBI systems have emerged among political actors as a result of

both technical developments in the field and early legislative activity of EU institutions: 1) active promotion 2) support with safeguards; 3) moratorium and 4) outright ban.
Those who are in favour of support with safeguards argue that the deployment RBI technologies should be strictly monitored because of the potential risks they pose, including the potential danger of FRT, for example, to contribute to the further criminalisation or stigmatisation of groups of people who already face discrimination.

The European Parliament passed a resolution on artificial intelligence in January 2020 in which they invite the Commission "to assess the consequences of a moratorium on the use of facial recognition systems". If deemed necessary, such a moratorium could impact some existing uses of FRT including its deployment in public spaces by public authorities.
A number of EU and national NGOs have called for an outright ban on the use of RBI with some arguing that the mass processing of biometric data from public spaces creates a serious risk of mass surveillance that infringes on fundamental rights.

The European Commission's legislative proposal for an Artificial Intelligence Act (EC 2021) is both a proposal for a regulatory framework on AI and a revised coordinated plan to support innovation. One feature of the act is the establishment of risk-dependent restrictions which would apply to the various uses of AI systems.

CASE STUDIES

CHAPTER 6: FACIAL RECOGNITION CAMERAS AT BRUSSELS INTERNATIONAL AIRPORT (BELGIUM)

Belgium is one of two European countries that has not yet authorised the use of FRT, however, law enforcement is strongly advocating for its use and the current legal obstacles to its implementation are unlikely to hold for very long. In 2017, unbeknownst to the Belgian Supervisory Body for Police Information (COC), Brussels International Airport acquired 4 cameras connected to a facial recognition software for use by the airport police. Though the COC subsequently ruled that this use fell outside of the conditions for a lawful deployment, the legality of the airport experiment fell into a legal grey area because of the ways in which the technology was deployed.

One justification for the legality of the airport experiment from the General Commissioner of Federal Police was to compare the technological deployment to that of the legal use of other intelligent technologies such as Automated Number Plate Recognition (ANPR). Although this argument was rejected at the time, such a system could be re-instated if the grounds for interruption are no long present in the law.
There is an emerging civil society movement in Belgium contesting the legitimacy of remote biometric identification. However, the amendments to the Police Act permitting the use of real-time smart cameras by the police in carrying out their administrative and judicial duties, and recent declarations of the Minister of Interior seems to point in the direction of more acceptance for remote biometric surveillance.

CHAPTER 7: THE BURGLARY FREE NEIGHBOURHOOD IN ROTTERDAM (NETHERLANDS)

The Fieldlab Burglary Free Neighbourhood is a public-private collaboration with two aims: to detect suspicious behaviour and to influence the behaviour of the suspect. While the system of smart streetlamps does collect some image and sound-based data, it does not record any characteristics specific to the individual.

From a legal perspective, there is a question as to whether or not the data processed by the Burglary Free Neighbourhood programme

qualifies as personal data and thus would fall within the scope of data protection legislation. It is contested whether forms of digital monitoring and signalling are actually the most efficient methods for preventing break ins. Despite the aims of the programme, to date, the streetlights have only been used to capture data for the purposes of machine learning.
The infrastructure installed for the experiments can potentially be used for more invasive forms of monitoring. During the project, local police, for example, already voiced an interest in access to the cameras.

In March 2021, the Fieldlab trial ended. The data collected over the course of the project was not sufficient enough to have the computer distinguish suspicious trajectories. The infrastructure of cameras and microphones is currently disabled, yet remains in place.

CHAPTER 8: THE SAFE CITY PROJECTS IN NICE (FRANCE)

Several French cities have launched "safe city" projects involving biometric technologies, however Nice is arguably the national leader. The city currently has the highest CCTV coverage of any city in France and has more than double the police agents per capita of the neighbouring city of Marseille.

Through a series of public-private partnerships the city began a number of initiatives using RBI technologies (including emotion and facial recognition). These technologies were deployed for both authentication and surveillance purposes with some falling into the category of biometric mass surveillance.

One project which used FRT at a high school in Nice and one in Marseille was eventually declared unlawful. The court determined that the required consent could not be obtained due to the power imbalance between the targeted public (students) and the public authority (public educational establishment). This case highlights important issues about the deployment of biometric technologies in public spaces.
The use of biometric mass surveillance by the mayor of Nice Christian Estrosi has put him on a collision course with the French Data Protection Authority (CNIL) as well as human rights/ digital rights organisations (Ligue des Droits de l'Homme, La Quadrature du Net). His activities have raised both concern and criticism over the usage of the technologies and their potential impact on the privacy of personal data.

CHAPTER 9: FACIAL RECOGNITION IN SÜDKREUZ BERLIN, HAMBURG G20 AND MANNHEIM (GERMANY)

The German federal police, in cooperation with the German railway company, conducted a project called "Sicherheitsbahnhof" at the Berlin railway station Südkreuz in 2017/18, which included 77 video cameras and a video management system.

The police in Hamburg used facial recognition software Videmo 360 during the protests against the G20 summit in 2017. The database includes 100.000 individuals in Hamburg during the G20 summit and whose profiles are saved in the police database. The technology allows for the determination of behaviour, participation in gatherings, preferences, and religious or political engagement.

Sixty-eight cameras were installed by local police on central squares and places in the German city Mannheim to record the patterns of movement of people. In this project, which started in 2018, the software is used to detect conspicuous behaviour.
Half of these deployments (Mannheim & Berlin Südkreuz) took place as measures to test the effectiveness of facial recognition and behavioural analysis software. This "justification as

a test" approach is often used in Germany to argue for a deviation from existing rules and societal expectations and was similarly applied during deviations to commonly agreed measures in the Coronavirus/COVID-19 pandemic.

Resistance to video surveillance is also in no small part a result of constant campaigning and protest by German civil society. The Chaos Computer Club and Digital Courage have consistently campaigned against video surveillance and any form of biometric or behavioural surveillance. The long-term effect of these "pilots" is to normalise surveillance.

CHAPTER 10: THE DRAGONFLY PROJECT (HUNGARY)

The Hungarian Government led by Prime Minister Viktor Orbán has long been on a collision course with EU Institutions over the rule of law and the undermining of the country's judicial independence and democratic institutions.

Hungary is a frontrunner in Europe when it comes to authorising law enforcement's use of Facial Recognition Technology, developing a nationwide and centralised database (The Dragonfly Project), and using the Home Quarantine App as part of the Government's Coronavirus measures.

The infrastructure in place that potentially allows for a centralised deployment of biometric mass surveillance technologies in Hungary has reached an unprecedented scale while the legal and ethical scrutiny of these technologies lags dangerously behind.

This is due to (1) the overlap between the private and public sectors, specifically government institutions, and (2) the complex entanglements biometric systems have with other information systems (such as car registries, traffic management, public transport monitoring and surveillance, etc.).

Although the latter are not concerned with the traces of the human body they can nonetheless be used for and facilitate biometric mass surveillance. These entanglements create grey zones of biometric mass surveillance where the development and deployment of such technologies is hidden from visibility and critical scrutiny.

The Dragonfly Project has elicited numerous warnings regarding data protection and the rights to privacy from both public and private organisations. However the lack of contestation and social debate around the issues of privacy and human rights in relation to such projects as the Hungarian Government's Dragonfly is striking.

CHAPTER 11: RECOMMENDATIONS

1. The EU should prohibit the deployment of both indiscriminate and "targeted" Remote Biometric and Behavioural Identification (RBI) technologies in public spaces (real-time RBI), as well as ex-post identification (or forensic RBI). Our analysis shows that both practices, even when used for "targeted surveillance" amount to mass surveillance.

In line with similar recommendations made by the EDPB and the EDPS[1], the EU should prohibit the deployment of Remote Biometric and Behavioural Identification technologies in public spaces.

In line with the position of the EDRi regarding's EU Artificial Intelligence Act[2], our research supports the notion that the distinction between "real-time" and "ex-post" is irrelevant when it comes to the impact of these technologies on fundamental rights. Ex-post identification carries in fact a higher potential of harm, as more data can be pooled from different sources to proceed to the identification. The use of such technologies for "targeted sur-

1 https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en

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

veillance" is thus equally harmful as the practice might be considered as expansive and intrusive to an extent that it would constitute disproportionate interference with the rights to privacy and personal data protection.
This concerns not only the acquisition and processing of faces, but also gait, voice and other biometric or behavioural signals.

2. The EU should strengthen transparency and accountability of biometric and behavioural recognition technologies.
Our research found that the majority of surveillance systems remain opaque. There is very little information on how citizens' data is processed when they enter surveilled public spaces. Rarely are concrete alternatives provided if they do not wish to be surveilled. In some extreme cases, such as the deployment of FRT trials in London, citizens who deliberately avoided surveillance by covering their faces were subjected to fines. This poses considerable challenges to citizens' rights, as well as to transparency and accountability of these systems.

It seems thus necessary to **expand existing transparency and accountability requirements** in the new EU Artificial Intelligence Act for biometric technologies. These requirements should be expanded to include external independent accountability, transparency and oversight for any implementations of biometric technologies that are not already prohibited by the Act.

In particular, it seems imperative to increase the transparency of such systems, by conditioning their operation to the publication of key characteristics and features (type of data acquisition, type of machine learning algorithm, nature of data collected in the database) necessary for effective public oversight of their operation. These details should be disclosed even when deployments are used for national security or law enforcement purposes, and the public should be informed about planned and ongoing projects.

3. The EU should promote the reinforcement of robust accountability mechanisms for biometric surveillance systems.

The current legislative framework remains unclear as to which institutions may review or authorise biometric surveillance systems. In light of the GDPR and the LED, the Data Protection Authorities (DPAs) in some member states enforce the relevant data protection legislation and oversee the processing of biometric data, while in others a separate authority is tasked with the responsibility to review the compatibility with the relevant legislation insofar as personal data processing by law enforcement authorities is concerned (such as Belgium, see case study).

The EU should work toward developing a centralised authorisation process for biometric surveillance, within which all relevant authorities are included and are able to veto the authorisation.

Although the proposed EU Artificial Intelligence Act limits a prior authorisation by a court or independent administrative authority to 'real-time' biometric surveillance, it is necessary to underline that ex-post biometric identification systems must be subject to supervision or authorisation taking into account the standards under the ECHR and the Charter.

4. The EU should promote individual rights under the GDPR through the promotion of digital-rights-by-design technologies.
More attention could be given to protect individuals' rights under GDPR when it comes to data collection and processing mechanisms as well as a fundamental rights assessment ex ante and ex post.

This could be implemented technically through data minimisation or digital rights-by-design methods, either through technical solutions that do not collect biometric information, or systems which incorporate automated forms of notification, immutable transparency and accountability logging, and control of data or ideally by a combination of both approaches.

5. The EU should ensure effective enforcement of GDPR purpose limitation.
Purpose limitation is one of the key principles of the GDPR. As our report shows, the re-purposing of biometric data is not always kept sufficiently in check.

From a technical perspective, biometric mass surveillance can easily emerge by connecting different elements of a technical infrastructure (video acquisition capacities, processing algorithms, biometric datasets) developed in other contexts.

For example, while the forensic use of facial recognition is not a form of remote biometric identification per se, the adoption of such systems has allowed for the creation of biometrically searchable national datasets. These datasets are one piece of a potential biometric mass surveillance infrastructure which can become a technical reality if live camera feeds, processed through live facial recognition software is connected to them.

In order to maintain democratic oversight over the uses of the infrastructure, and avoid the risk of function creep (i.e. when a technology is being used beyond its initial purpose) it is thus imperative that the principle of purpose limitation is systematically enforced and strictly regulated with regard to the type of data (criminal or civilian datasets, datasets generated from social media, as in the Clearview AI controversy) against which biometric searches can be performed.
6. The EU should support voices and organisations which are mobilised for the respect of EU fundamental rights.

Finally, our research showed, in addition to state oversight agencies, many institutions from civil society are active in making sure that EU fundamental rights are respected in the field of biometric security technologies.
While in some countries they benefit from a dense network of civil society funding, in others they are subjected to heavy scrutiny and financial restrictions (see for example the Hungary case study in this report).
Supporting civil society organisations that operate in the sector of digital rights is therefore instrumental for a healthy democratic debate and oversight. Civil society need to be able to participate in all relevant legislative and other decision-making procedures.

Particularly in the area of litigation, support for civil society and EU citizens access to rights could be extremely helpful. We have found numerous areas in our study where sufficient legal clarity was lacking and would likely only take place through the courts. We would thus advise that the EU support existing digital rights litigation initiatives and create additional mechanisms to support this approach.

7. The EU should take into account the global dimension of the Biometric and Behavioural Analysis Technology Industry.
The technologies used for FRT in Europe come from vendors across the world. Technologies for biometric or behavioural analysis are often tested in one country before they are implemented in another.
EU policy on the biometric or behavioural analysis technology industry thus needs to consider its impact both inside and outside of Europe. Here, the recently revised EU Export Control framework which may include biometric and behavioural technologies can play a role.

CHAPTER 1
INTRODUCTION

INTRODUCTION

Key points

- The aim of this report is to establish a problematised overview of what is currently being done in Europe when it comes to remote biometric identification (RBI), and to assess in which cases we could potentially fall into forms of biometric mass surveillance.
- Private and public actors are increasingly deploying “smart surveillance” solutions including RBI technologies which, if left unchecked, could become biometric mass surveillance.
- Facial recognition technology has been the most discussed of the RBI technologies. However, there seems to be little understanding of the ways in which this technology might be applied and the potential impact of such a broad range of applications on the fundamental rights of European citizens.
- The development of RBI systems by authoritarian regimes which may subsequently be exported to and used within Europe is of concern. Not only as it pertains to the deployments of such technologies but also the lack of adequate insight into the privacy practices of the companies supplying the systems.
- Four main positions have emerged with regard to the deployments of RBI technologies and their potential impact on fundamental rights: 1) active promotion 2) support with safeguards; 3) moratorium and 4) outright ban.

Since the widespread use of neural network algorithms in 2012, artificial intelligence applied to the field of security has steadily grown into a political, economic, and social reality. As examples from Singapore, the UK, South Africa, or China demonstrate, the image of a digital society of control, in which citizens are monitored through algorithmically processed audio and video feeds is becoming a tangible possible reality in the European Union.

Through a set of "pilot projects", private and public actors including supermarkets, casinos, city councils, border guards, local and national law enforcement agencies are increasingly deploying a wide array of "smart surveillance" solutions. Among them remote biometric identification, namely security mechanisms "that leverage unique biological characteristics" such as fingerprints, facial images, iris or vascular patterns to "identify multiple persons' identities at a distance, in a public space and in a continuous or ongoing manner by checking them against data stored in a database." (European Commission 2020b, 18) European institutions have reacted with a series of policy initiatives in the last years, but as we will show in this report, if left unchecked, remote biometric identification technologies can easily become biometric mass surveillance.

Among technologies of remote biometric identification, facial recognition has been at the centre of the attention of most discussions in the public debate. The foregrounding of this specific use case of computer vision in the public debate has allowed concerned actors to raise awareness on the dangers of artificial intelligence algorithms applied to biometric datasets. But it has also generated confusion. The perception that facial recognition is a single type of technology (i.e., an algorithm "that recognises faces") has obscured the broad range of applications of "smart technologies" within very different bureaucratic contexts: from the "smart cities" live facial recognition of video feeds deployed for the purpose of public space surveillance, to the much more specific, on-the-spot searches by law enforcement for the purpose of carrying out arrests or forensic investigations.

The disentanglement and specification of each of these uses is important, if only because each distinct technological arrangement between sensing devices (cameras, microphones), datasets and algorithmic processing tools allows for radically different applications, and thus can have different types of impact on European citizens' fundamental rights. As the recent communication of the European Commission (2021) stated, not all systems and not all applications are equally threatening for our democratic freedoms: some bear too much risk of infringing our fundamental rights – and therefore should never be allowed; some are "high risk" applications that can take place in certain circumstances with very clear safeguards; and some are more mundane uses of the technologies that require less attention. The ethical, political, and legal assessment of these levels of danger can therefore not be separated from a detailed understanding of how these technologies work. The limitation being of course that while we know what technologies are theoretically available to public actors, the detail of their characteristics is often hidden from view.

OBJECTIVES OF THE REPORT

The aim of this report is thus to establish a problematised overview of what we know about what is currently being done in Europe when it comes to remote biometric identification, and to assess in which cases we could potentially fall into forms of biometric mass surveillance. The report will thus answer the following questions: What types of technologies are being used and how? In what context? By whom are these technologies used and to

what aim? What types of actors are involved? What types of consequences does the use of those technologies entail? What legal basis and framework are applied to the use of those technologies? What are the forms of mobilisation and contestation against these uses?

In the rest of this introduction, we locate the political context for this study, including the voices that have called for a moratorium or a ban of all technologies that are associated with "biometric mass surveillance". We then specify the objectives, scope, methodology, some working definitions and outline the remaining chapters.

THE INTERNATIONAL CONTEXT

The concern for uncontrolled deployment of remote biometric identification systems emerges in a context characterised by the development of technologies in authoritarian regimes; the development of controversial "pilot" projects as part of "smart cities projects" in Europe; revelations about controversial privacy practices of companies such as Clearview AI; and finally, by the structuration of a US and EU debate around some of the key biases and problems they entail.

In 2013, the Chinese authorities officially revealed the existence of a large system of mass surveillance involving more than 20 million cameras called Skynet, which had been established since 2005. While the cameras were aimed at the general public, more targeted systems were deployed in provinces such as Tibet and Xinjiang where political groups contest the authority of Beijing. In 2018, the surveillance system became coupled with a system of social credit, and Skynet became increasingly connected to facial recognition technology (Ma 2018; Jiaquan 2018). By 2019, it was estimated that Skynet had reached 200 million face-recognition enabled CCTV cameras (Mozur 2018).

The intrusiveness of the system, and its impact on fundamental rights is best exemplified by its deployment in the Xinjiang province. The province capital, Urumqi, is chequered with checkpoints and identification stations. Citizens need to submit to facial recognition ID checks in supermarkets, hotels, train stations, highway stations and several other public spaces (Chin and Bürge 2017). The information collected through the cameras is centralised and matched against other biometric data such as DNA samples and voice samples. This allows the government to attribute trust-worthiness scores (trustworthy, average, untrustworthy) and thus generate a list of individuals that can become candidates for detention (Wang 2018).

European countries' deployments are far from the Chinese experience. But the companies involved in China's pervasive digital surveillance network (such as Tencent, Dahua Technology, Hikvision, SenseTime, ByteDance and Huawei) are exporting their know-how to Europe, under the form of "safe city" packages. Huawei is one of the most active in this regard. On the European continent, the city of Belgrade has for example deployed an extensive communication network of more than 1.000 cameras which collect up to 10 body and facial attributes (Stojkovski 2019).

The cameras, deployed on poles, major traffic crossings and a large number of public spaces allow the Belgrade police to monitor large parts of the city centre, collect biometric information and communicate it directly to police officers deployed in the field. Belgrade has the most advanced deployment of Huawei's surveillance technologies on the European continent, but similar projects are being implemented by other corporations – including the European companies Thales, Engie Ineo or Idemia – in other European cities and many "Safe City" deployments are planned soon

in EU countries such as France, Italy, Spain, Malta, and Germany (Hillman and McCalpin 2019). Furthermore, contrary to the idea China would be the sole exporter of Remote Biometric Identification technologies, EU companies have substantially developed their exports in this domain over the last years (Wagner 2021)

The turning point of public debates on facial recognition in Europe was probably the Clearview AI controversy in 2019-2020. Clearview AI, a company founded by Hoan Ton-That and Richard Schwartz in the United States, maintained a relatively secret profile until a New York Times article revealed in late 2019 that it was selling facial recognition technology to law enforcement. In February 2020, it was reported that the client list of Clearview AI had been stolen, and a few days later the details of the list were leaked (Mac, Haskins, and McDonald 2020). To the surprise of many in Europe, in addition to US government agencies and corporations, it appeared that the Metropolitan Police Service (London, UK), as well as law enforcement from Belgian, Denmark, Finland, France, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Norway, Portugal, Serbia, Slovenia, Spain, Sweden, and Switzerland were on the client list. The controversy grew larger as it emerged that Clearview AI had (semi-illegally) harvested a large number of images from social media platforms such as Facebook, YouTube and Twitter in order to constitute the datasets against which clients were invited to carry out searches (Mac, Haskins, and McDonald 2020).

The news of the hacking strengthened a strong push-back movement against the development of facial recognition technology by companies such as Clearview AI, as well as their use by government agencies. In 2018, Massachusetts Institute of Technology (MIT) scholar and Algorithmic Justice League founder Joy Buolamwini together with Temnit Gebru had published the report Gender Shades (Buolamwini and Gebru 2018), in which they assessed the racial bias in the face recognition datasets and algorithms used by companies such as IBM and Microsoft. Buolamwini and Gebru found that algorithms performed generally worse on darker-skinned faces, and in particular darker-skinned females, with error rates up to 34% higher than lighter-skinned males (Najibi 2020). IBM and Microsoft responded by amending their systems, and a re-audit showed less bias. Not all companies responded equally. Amazon's Rekognition system, which was included in the second study continued to show a 31% lower rate for darker-skinned females.The same year ACLU conducted another key study on Amazon's Rekognition, using the pictures of members of congress against a dataset of mugshots from law enforcement. 28 members of Congress, largely people of colour were incorrectly matched (Snow 2018).

A number of organizations seized the problem as a policy issue (Black in AI, Algorithmic Justice League, Data for Black Lives) and some engaged lawmakers. In 2019, the Algorithmic Accountability Act allowed the Federal Trade Commission to regulate private companies' uses of facial recognition. In 2020, several companies, including IBM, Microsoft, and Amazon, announced a moratorium on the development of their facial recognition technologies. Several US cities, including Boston, Cambridge (Massachusetts) San Francisco, Berkeley, Portland (Oregon), have also banned their police forces from using the technology.

THE EUROPEAN CONTEXT

In Europe, a similar set of developments took place around Artificial Intelligence in activist circles, both at the member states level and at the EU level. (Andraško et al. 2021, 3). The first intervention dates from 2017 with the European Parliament Resolution of 16 February to the Commission on Civil Law Rules on Robotics

(European Parliament 2017). It was followed by two statements and advisory documents: The Age of Artificial Intelligence, published by the European Political Strategy Centre; and a Statement on Artificial Intelligence, Robotics and Autonomous Systems (March 2018), published by the European Group on Ethics in Science and New Technologies (Andraško et al. 2021, 3). At the beginning of 2018, the European Economic and Social Committee issued three opinions on the deployment of AI in practice (European Economic and Social Committee 2018a, 2018b, 2018c). All these documents addressed the need for the EU to understand AI uses, and embedded them in the various ethical and political frameworks created by EU institutions. The same year, the Council of Europe began its activities on the matter. In 2017, the Parliamentary Assembly of the Council of Europe adopted a Recommendation on Technological Convergence, Artificial Intelligence and Human Rights pointing towards the need to established common guidelines for the use of artificial intelligence in court (Parliamentary Assembly of the Council of Europe 2017; Gonzalez Fuster 2020, 45).

Legislative activity accelerated in 2018. The European Commission (2018a) published a communication Artificial Intelligence for Europe, in which it called for a joint legal framework for the regulation of AI-related services. Later in the year, the Commission (2018b) adopted a Coordinated Plan on Artificial Intelligence with similar objectives. It compelled EU member states to adopt a national strategy on artificial intelligence which should meet the EU requirements. It also allocated 20 billion euros each year for investment in AI development. (Andraško et al. 2021, 4).

In 2019, the Council of Europe Commissioner for Human Rights published a Recommendation entitled Unboxing Artificial Intelligence: 10 steps to Protect Human Rights which describes several steps for national authorities to maximise the potential of AI while preventing or mitigating the risk of its misuse. (Gonzalez Fuster 2020, 46). The same year the European Union's High Level Expert Group on Artificial Intelligence (AI HLEG) adopted the Ethics Guidelines for Trustworthy Artificial Intelligence, a key document for the EU strategy in bringing AI within ethical standards (Nesterova 2020, 3).

In February 2020, the new European Commission went one step further in regulating matters related to AI, adopting the digital agenda package – a set of documents outlining the strategy of the EU in the digital age. Among the documents the White Paper on Artificial Intelligence: a European approach to excellence and trust captured most of the commission's intentions and plans.

FOUR POSITIONS IN THE POLICY DEBATES

Over the past 3-4 years, positions around the use of facial recognition and more specifically the use of remote biometric identification in public space have progressively crystalised into four camps (for a more detailed analysis of the positions, see Chapter 5).

Active promotion

A certain number of actors, both at the national and at the local level are pushing for the development and the extension of biometric remote identification. At the local level, figures such as Nice's (France) mayor Christian Estrosi have repeatedly challenged Data Protection Authorities, arguing for the usefulness of such technologies in the face of insecurity (for a detailed analysis, see chapter 8 in this report, see also Barelli 2018). At the national level, Biometric systems for the purposes of authentication are increasingly deployed for forensic applications among law-enforcement agencies in the European Union. As we elaborate in Chapter 3, 11 out of 27 member states

of the European Union are already using facial recognition against biometric databases for forensic purposes and 7 additional countries are expected to acquire such capabilities in the near future. Several states that have not yet adopted such technologies seem inclined to follow the trend, and push further. Former Belgian Minister of Interior Pieter De Crem for example, recently declared he was in favour of the use of facial recognition both for judicial inquiries but also for live facial recognition, a much rarer instance. Such outspoken advocates of the use of RBI constitute an important voice, but do not find an echo in the EU mainstream discussions.

Support with safeguards

While there is little widespread support for the development of centralised biometric mass surveillance, some actors such as the European Council and the European Commission have advocated a cautious and regulated development of remote biometric identification systems, as part of a broader Artificial Intelligence strategy. The principles of such strategies have been outlined in the various strategy documents discussed above. A large number of the technology companies are hoping that this position remains the main one, with many of them eager to implement the ethical requirements necessary for the deployments of their systems. In addition to the political and legislative activity mentioned above, the EU institutions have been active in promoting the use of Artificial Intelligence and biometric surveillance technologies. As detailed in chapter 5, instruments such as the Digital Europe programme, the Connecting Europe Facility 2 and Horizon Europe will form the basis for collaboration between public institutions and the security industry developing biometric remote identification products. In the European Parliament, positions are divided and moving, but parties like the European People Party support a similar notion of careful development.

Moratorium

For other actors, such as the European Parliament or the Council of Europe, remote biometric identification systems entail too many unknown risks and thus need to be put on hold. The proponents of a moratorium invoke the necessity of applying the principle of precaution – a similar strategy to opponents of the commercialisation of GMO in Europe – so that all dimensions of the technology can be assessed before a decision can be made. On 20 January 2021, the European Parliament passed a resolution inviting the EU Commission to consider a moratorium on the use of facial recognition systems (European Parliament 2021). Similarly, in 2021, the Council of Europe (2021) adopted Guidelines on Facial Recognition (Council of Europe, 2021) which call for a moratorium for the live facial recognition technologies and lay out certain conditions for the use of facial recognition technologies by law enforcement authorities.)

Ban

Finally, a growing number of actors considers that there is enough information about remote biometric identification in public space to determine that they will never be able to comply to the strict requirement of the European Union in terms of respect of Fundamental Rights, and as such should be banned entirely. It is the current position of the European Data Protection Supervisor (EDPS, 2021) the Council of Europe and a large coalition of NGOs (among which La Quadrature du Net and the collaborative project Technopolice,) gathered under the umbrella of the European Digital Rights organisation (EDRi 2020). In the European Par-

liament, the position has most vocally been defended by the European Greens, but has been shared by several other voices, such as members of the Party of the European Left, the Party of European Socialists or Renew Europe (Breyer et al 2021).

LACK OF TRANSPARENCY AND THE STIFLING OF PUBLIC DEBATE

An additional important question concerns the reaction of the public at large. While the development of face recognition technologies and more broadly remote biometric identification systems has elicited stark responses from watchdogs, civil liberties unions and human rights activist (CNIL 2019b; EDRi 2020; Renaissance Numérique 2019; Gonzales Fuster 2020), the state of the debate and awareness in the wider public is actively muddled by a lack of transparency in how these technologies are developed and implemented, both by private companies and public authorities.

This lack of transparency, and sometimes secrecy surrounding some of the technological parameters is not casual: "vendors of facial recognition software might not want to disclose information about the training data, as was experienced by an expert from a civil society organization" warns the FRA (2019, 10). Copyright issues and trade secrets are invoked to also block access to information that would be needed to assess the quality of systems employed. Governments, at the national or local level, invoke national security concerns in order to remain opaque about the deployment of the technologies, the contracted parties (See Chapter 10) and citizens often found out about their implementation after the fact (see Chapter 6). Finally, the societal debate about these issues is further hindered by the porosity between the public and private dimensions of these technologies. Users often willingly volunteer their biometric data, and do not always perceive the technical differences that might exist between unlocking their phones through facial recognition (the data remains in a separate chip on the phone) and using applications which leak biometric information in remote databases, making them available not only to commercial vendors, governments, law enforcements authorities, but hackers and other actors interested in the misuse of this data.

For these reasons, informed political debate cannot take place without a thorough effort of digital literacy concerning the development of these new technologies. But it will also rely on information being made available to the public, so that the parties involved can be held accountable and the impact of technologies on the everyday life of European citizens can be critically assessed. The aim of this report is thus precisely to present evidence about the remote biometric identification technologies, the current state of their deployment in Europe as well as their ethical, social, and political implications to provide context and recommendation on the various positions.

SCOPE AND WORKING DEFINITIONS

This report will be centred on "biometric and behavioural mass surveillance" in public spaces. In addition to the definition of Remote Biometric Identification provided above, we define biometric data as all data related to the body, which can be used to identify or monitor individuals or groups of individuals and is impossible or very difficult to alter (face, fingerprints, iris, etc.). Behavioural data concerns the data collected related to the way in which individuals uniquely behave (facial expressions, body movements, voice, etc.). Finally, we define Biometric Mass Surveillance as a form of monitoring, tracking, or processing of personal (biometric and behavioural) data of individuals indiscriminately and in a generalised manner without a prior criminal suspicion (FRA, 2019). We can add that this surveillance

occurs at a distance, in a public space and in a continuous or ongoing manner by checking them against data stored in a database. We thus conceptualise biometric mass surveillance, if left unchecked, as the possible dystopian horizon of remote biometric identification technologies.

The report will primarily focus on those technologies (facial recognition, voice recognition, and the classification of behaviour) that are deployed in EU public spaces. It will initially focus on the deployment of such technologies by public actors in public spaces in the EU, such as cities. Public spaces can be publicly owned (roads, streets, city squares, parking facilities, government facilities) or privately owned (shopping malls, stadiums). Similarly, private actors can deploy these technologies in public spaces in collaboration with, or for further use by, public actors (e.g., the use of private Amazon Ring footage collected by individuals and shared with the police in some US cities).

On the basis of these specifications, the following cases are being excluded from the analysis: deployment of remote biometric identification technologies by private actors in private spaces (one's house) if such deployments have no public consequences; deployment of remote biometric identification technologies created by EU companies used outside of the EU (exports); deployment of remote biometric identification outside of EU public spaces (such as surveillance of the EU borders in the Mediterranean). Further technical definitions are provided in CHAPTER 2.

METHODOLOGY

This report is based primarily on desk research. It is based on primary sources from international and regional organisations, national governments, local authorities, non-governmental organizations and private companies, as well as secondary sources (academic literature). For some of the case studies qualitative interviews were carried out remotely (via telephone or video-call) and are indicated as such. For the dataset used in the related interactive map, we are particularly grateful to the Technopolice project and to Felix Tréguer for helping us accessing the data already collected for France. The report was commissioned in February 2021 and was written between February 2021 and October 2021.

PART 1

OVERVIEW OF EUROPEAN PRACTICES

CHAPTER 2

TECHNICAL OVERVIEW

OVERVIEW OF **EUROPEAN PRACTICES**

TECHNICAL OVERVIEW

Key points

- The current market of RBI systems is overwhelmingly dominated by image-based products, at the centre of which is facial recognition technology (FRT). Other products such as face detection and person detection technologies are also in use.
- FRT is typically being deployed to perform two types of searches: cooperative searches for verification and/ or authentication purposes, and non-cooperative searches to identify a data subject. The former involves voluntary consent from the data subject to capture their image, while the latter may not.
- Live facial recognition is currently the most controversial deployment of FRT: Live video feeds are used to generate snapshots of individuals and then match them against a database of known individuals – the “watchlist”.
- Other RBI technologies are being deployed though their use at present is marginal compared to FRT, these include gait, audio, and emotion recognition technologies, amongst others.
- A better understanding of the technical components and possible usage applications of image-based RBI technologies is needed in order to assess their potential political implications.
- RBI technologies are subject to technical challenges and limitations which should be considered in any broader analysis of their ethical, legal, and political implications.

In order to grasp the various facets of remote biometric identification that could potentially lead to biometric mass surveillance, this section provides an overview of the currently available technologies, how they work and what their limitations are as well as where and by whom they are deployed in the European Union.

REMOTE BIOMETRIC IDENTIFICATION AND CLASSIFICATION: DEFINING KEY TERMS

Although there are a growing number of technologies based on other supports than images (photographs or videos) such as voice recognition (audio), LIDAR scans or radio waves, the current market of remote biometric identification is overwhelmingly dominated by image-based products, at the centre of which is face recognition. In the following sections we thus focus primarily on image-based products.

DETECTION VS RECOGNITION

- Person detection denotes the ability of a software application to estimate (as in, provide a statistical probability) whether an object in the camera image is a person. Generally, it is able to indicate the position of the person in the image. Person detection systems can be used in basic analytics scenarios, where for example the presence of people is counted. Moreover, object detection algorithms can be used to track individuals between video frames, although they generally have a hard time tracking occlusions (people walking in front of others, hiding them from the camera) and specific people across multiple camera viewpoints. Person detection does not obtain any information about individuals faces.
- Face detection, similar to person detection, refers to the capacity of a software application to detect that an object in the field of view of a camera is a human face. It is the most familiar function of smart technologies: it has been present in consumer electronics, such as photo cameras and mobile phones for years. Face detection provides the recognisable rectangle around faces when taking a picture with a smart phone. Similarly, it can be used in surveillance applications to assess the presence or positions of individuals.

- Facial recognition builds on top of face detection. The software uses the detected faces to determine who is in the picture. In order to do so, an algorithm calculates a numerical representation of the detected face, called a “feature vector” or “embedding”. This vector, which is unique to each individual, is what allows systems to perform searches. The detected vector can for example be used to search for existing identical vectors in a database of known individuals, where vectors are related to an identity. In a different type of usage, the feature vector can be used to track people moving from one camera’s field of view to the next. In this case, the vector is not used to find a “match” in a database but serves instead to confirm that it is the same individual that appears in different camera feeds.

FACIAL RECOGNITION: VERIFICATION/ AUTHENTICATION VS IDENTIFICATION

Within the domain of facial recognition, two general types of searches are performed.

- One-to-one (1:1) searches are called verification or authentication searches and are used to determine whether an individual face presented to the camera matches a single face stored in the system. This is how “Face ID” works on iPhones for example. In this example, people volunteer the capture of their face, they are thus considered in a “cooperative” scenario.

- One-to-many (1:N) searches are called identification searches. An unknown single face, picked up for example from surveillance video footage or from a passport, is run aga-

inst a large dataset of known faces, in order to identify the unknown face, or to determine if it occurs on a so called "watchlist". This can be done in the case of forensic investigations or can be deployed in remote biometric identification scenarios in the public space. In this latter example, when faces are captured without the intention or consent of the individuals, the capture is considered "non-cooperative". Because of the larger amount of data, identification is from a technical perspective, substantially more difficult to perform than authentication. As such, many of these implementations do not return a single identity upon request, but rather provide a list of likely identities with, for example, a match likeliness score. Note that identification does not automatically entail the recoding of the name of the individual in the database. For example, if visitors of a shop are recorded, the software can look for recurring visitors without having their names.

FORENSIC (EX-POST) VS LIVE FACIAL RECOGNITION

A final distinction can be made between forensic (or ex-post) and live facial recognition. Forensic facial recognition is carried out generally in the context of judicial investigations in order to match photographs of persons of interest captured via surveillance cameras or extracted from documents to an operational database of known individuals (Al-Kawaz et al. 2018). It is the most commonly use type of facial recognition in Europe, in particular by law enforcement authorities. Live facial recognition, instead, uses live video feeds in order to generate snapshots of individuals and then match them against a database of known individuals – the "watchlist". It is the most controversial deployment of facial recognition (Fussey and Murray 2019).

OTHER SYSTEMS: GAIT RECOGNITION, EMOTION RECOGNITION

Facial recognition occupies the central stage of the discussion when it comes to remote biometric identification and classification, because it is simply the most mature technology. Yet other technologies should be mentioned, in particular when considering biometric classification. They are for the moment relatively marginal, and information about their deployment is anecdotal at this stage.

Gait recognition

Gait recognition consists of recognising the specific way in which a person walks (gait), but in reality it covers a broader range of criteria (body, proportions, posture, etc.) (Segal 2020, 2). The advantages of gait recognition are that it does not require a clear access to a face, and it requires a lower image resolution (as it analyses an entire body, not only a face). Gait recognition, however, requires more computing power because it works on the basis of moving images (i.e., multiple frames of still images, up to 30 frames per second) rather than still images. Gait recognition has been used as evidence in court for a case in Denmark (Segal 2020, 18). Gait recognition poses important technical challenges: The amount of data storage and processing power far exceeds that of facial recognition. There are currently very few training datasets. So far, systems have proven to be more expensive, and less accurate than facial recognition.

People tracking and counting

This is perhaps the form of person tracking with which the least information about an individual is stored. An object detection algorithm estimates the presence and position of individuals on a camera image. These positions are stored or counted and used for

further metrics. It is used to count passers-by in city centres, and for a one-and-a-half-meter social distancing monitor in Amsterdam[1]. See also the case study in this document on the Burglary-Free Neighbourhood in Rotterdam (CHAPTER 7), which goes into more detail about the use of the recorded trajectories of individuals to label anomalous behaviour.

Emotion recognition

Software that categorises facial expressions into emotion categories – happiness, sadness, anger, etc. – is known to be used in billboards that are equipped with cameras, in order to analyse audience response to advertisements. For example, in airports or at train stations. While the face is claimed to be a "window into the brain" by some, the technology has been heavily criticised. Firstly, some consider it an undesirable invasion of their privacy, while other critique the technology for capturing primarily stereotypical ways of expressing oneself (van de Ven, 2017). In some places, such as at Dutch train stations, these critiques have led to disabling the cameras in billboards altogether (Het Parool, 2017).

Age, gender, and ethnicity classification

Aside from deducing emotions, the face is used to deduce a variety of traits from individuals. For example, gender, ethnicity, and age estimations are available in many off-the-shelf facial analysis products. As with emotion recognition, these classifications are mainly used in digital signage and video advertisement contexts. LGBTQ+ communities have spoken out against automatic gender classification, pointing out that a long fought, non-binary understanding of gender is made undone by the technology's binary classifications (Vincent, 2021). Similarly, recent revelations that Hikvision (China) has used similar technology to estimate whether an individual is from China's Uyghur minority, has directly led the European Parliament to call for a ban of Hikvision's products on the Parliament's premises (Rollet, 2021).

Audio recognition

From a technological perspective, neural networks process audio relatively similarly to how video is processed: rather than feeding an image, a spectrogram is used as input for the network. However, under the GDPR, recording conversations, is illegal in the European Union without informed consent of the participants. In order to adhere to these regulations, on some occasions, only particular frequencies are recorded and processed. For example, in the Burglary-Free Neighbourhood in Rotterdam (Netherlands) (CHAPTER 7), only two frequencies are used to classify audio; making conversations indiscernible while being able to discern shouting or the breaking of glass[2]. Another initiative using audio in to enhance the surveillance camera is the Living Lab International Zone project in the Hague (Netherlands), a collaboration between a broad range of partners[3].

HOW DOES IMAGE-BASED REMOTE BIOMETRIC IDENTIFICATION WORK?

In order to assess the political implication of each of these systems, it is important to disaggregate the main technical components and understand the different possible technologies at play. Although the marketing of security companies uses the notion of "smart cameras", one should distinguish between the sensing hardware (cameras, microphones, LIDAR scanners) and the type of video analytics the captured data is subjected to. This second aspect should be further divided into an analy-

1 The one-and-a half meter monitor is trained on the COCO dataset, published by Microsoft and Facebook AI

2 Relatedly, see the Spotify controversy (Access Now 2021)

3 Partners in the Living Lab International Zone include: Municipality of The Hague, The Hague Police Region, TNO, Thales, Sorama, Connection Systems, Crowd Sense, The Hague Security Region, Europol, Eurojust, OPCW, IRMCT, Peace Palace, Catshuis, Government Buildings Agency, Ministry of Foreign Affairs and The Hague Security Delta.

sis of the training datasets and the algorithms.

Image acquisition: Controlled and uncontrolled images

Facial recognition begins with an image. An image which will be subject to the algorithm's scrutiny. Controlled images are images that are captured for the purpose of processing, aimed at optimal positions and lighting conditions. They are for example taken at a police station, or at a photographer's studio with strict requirements, and are either contained in databases that precede the introduction of a facial recognition system (e.g., driver's license databases) or are specifically designed to match high criteria of biometric systems (i.e., photographs for biometric passports). Uncontrolled images are images that are captured outside of specific requirement, collected for example through social media scraping or video surveillance.

When it comes to the acquisition technologies (cameras) for uncontrolled images, over the past decades, the main evolution in terms of video has been the passage from analogue video to digital video, the latter allowing images to be processed through computers. As in the realm of consumer cameras, the initial race was for better definition (calculated in terms of megapixels). "Smart" camera systems require a slightly higher resolution than standard video surveillance systems in order to guarantee a minimum of 300 PPM to adequately feed the software (IPVM Team 2020, 5). But overall, the average camera does not exceed a definition of 4 megapixels and are more often in the area of 2 megapixels (which yields a 1080p or HD resolution)[4]. The quality of capture, especially in non-cooperative scenarios, is determined by two main external variables: the angle of the face relative to the camera (front, side, back, top) and the lighting conditions (bright daylight, dark night). In recent years, manufacturers have added an additional infra-red channel to the red-green-blue (RGB) video channels in order to increase detail accuracy in low-light conditions.

What makes systems "smart": image processing algorithms

The processing of the photographic or video image by a specific software application is where the "smart" processing happens. Broadly speaking video surveillance technology can be split in two key historical moments: before machine learning, and after machine learning.

Video motion detection (VMD) and heuristic filters. The early smart technologies relied on simple motion detection algorithms which compared pixel changes from one image to the next (Quevillon 2012). The problem is that any movement (the leaves of a tree) or change of light (a car passing in the night) can trigger the systems. Heuristic filters were thus added to VMD systems in order to give additional parameters to the system (amount and size of pixel changing etc.). Both systems were highly inefficient and prone to trigger false alarms, making such technologies unattractive. The main problem was that only pre-established changes hard coded by humans would be detected by the systems.

Machine learning. Machine learning revolutionised image-based biometric identification. Machine learning is an automated process through which the software application will be programmed to recognise particular patterns, based on a dataset it is "trained" on. There are three ways in which this configuration of the machine learning model can be controlled: supervised, semi-supervised or unsupervised. Supervised machine learning consists of

4 For example, a in a 4K UHD image, composed of 3840 × 2160 pixels, a face occupying 300 x 300 pixels would need to occupy approximately 1/100 th of the screen's surface. In a HD image composed of 1920 x 1080 pixels, the same 300 x 300 pixel face would occupy about 1/25 th of the screen's surface.

teaching the system to recognise people, cars, guns, or any other object by feeding it an annotated dataset of such objects. It is supervised because humans "supervise" how the computer learns, by annotating the dataset ("this is a car", "this is a gun" etc.). The categories of the annotations (cars, guns, etc.) will thus be the only ones that the system will be able to recognise (if only cars and guns are annotated, the system won't in such a case recognise cats). Most video surveillance systems use supervised machine learning (IPVM Team 2021a, 11). Unsupervised machine learning lets the system cluster objects by itself. The advantage is the open-endedness of the systems (meaning they can generate categories of objects not anticipated in the training dataset), but the disadvantage is that algorithms can potentially cluster objects along irrelevant criteria for the task (for example clustering red motorcycles, cars, and trucks in one group and green ones in another, as opposed to creating one cluster for all motorcycles, one for cars and one for trucks). For this reason, semi-supervised machine learning, where only a small part of the data is labelled, can be used. Currently not widely in use, unsupervised machine learning is a growing trend in the video surveillance sector (IPVM Team 2021a, 12–13).

Both supervised and unsupervised learning exist in many shapes and sizes. For example, the Viola-Jones object detection algorithm[5] from 2001, which made real-time face detection viable, is a supervised algorithm. Contemporary developments in video processing focus on using various kinds of artificial neural networks (i.e., convolutional neural networks, recurrent neural networks) to classify images and videos. These networks can be trained either supervised, semi-supervised or unsupervised depending on their configuration.

Machine learning and operational datasets

Remote biometric identification and classification relies in large part on datasets, for two key but distinct moments of their operation.

Machine learning datasets. These are the datasets used to train models through machine learning. We find three categories of such datasets. Publicly available datasets for object detection such as COCO, ImageNet, Pascal VOC include a varying number of images labelled in a range of categories, these can be used to train algorithms to detect for example people on an image (IPVM Team 2021a, 27). The most used open-source datasets for surveillance technologies are Celeb 500k, MS-Celeb-1Million-Cleaned, Labeled Faces in the Wild, VGG Face 2, DeepGlint Asian Celeb, IMDB-Face, IMDB-Wiki, CelebA, Diveface, Flickr faces and the IARPA Janus Benchmark (IPVM Team 2021b, 7). Many of these datasets also function as a public benchmark, against which the performance and accuracy of various algorithms is measured. For example, Labeled Faces in the Wild, the COCO dataset and NIST present such leaderboards on their website[6]. Government datasets are generally collections of images available to a government for other purposes (driver's license, passport, or criminal record photo datasets). While in Europe most of these datasets are not accessible to the public, in China and in the US, they are made available for testing and training purposes to private companies, such as the Multiple Encounter Dataset (NIST, 2010). Finally proprietary datasets may be developed by providers for their specific applications.

Machine learning models. In the machine learning process, an algorithm gets iteratively configured for the optimal output, based on

5 "The Viola–Jones object detection framework is an object detection framework which was proposed in 2001 by Paul Viola and Michael Jones. Although it can be trained to detect a variety of object classes, it was motivated primarily by the problem of face detection." Wikipedia, "Viola–Jones object detection framework" https://en.wikipedia.org/wiki/Viola%E2%80%93Jones_object_detection_framework

6 See: http://vis-www.cs.umass.edu/lfw/results.html, https://cocodataset.org/#detection-leaderboard and https://www.nist.gov/programs-projects/face-challenges.

the particular dataset that it is fed with. This can be a neural network, but also e.g., the aforementioned Viola-Jones' object detector algorithm. The model is the final configuration of this learning process. As such, it does not contain the images of the dataset in and of themselves. Rather, it represents the abstractions the algorithm "learned" over time. In other words, the model operationalises the machine learning dataset. For example, the YOLO object detection algorithm yields different results when it is trained on either the COCO or the model (in conjunction with the algorithm) which determines the translation of an image into a category, or of the image of a face into its embedding.

Operational datasets, or image databases. Datasets used in training machine learning models should be distinguished from matching or operational datasets which are the "watchlists" of for example criminals, persons of interest or other lists of individuals against which facial recognition searches will be performed – whether these are in real time or post hoc. These datasets contain pre-processed images of individuals on the watchlist, and store the numerical representations of these faces, their feature vectors or embedding, in an index for fast retrieval and comparison with the queried features (using for example k-Nearest Neighbour or Support Vector Machines). Face or object detection models do not use such a dataset.

Availability

Facial recognition algorithms can be developed in-house, taken from an open-source repository, or purchased (IPVM Team 2021b, 14). Popular open-source facial recognition implementations include OpenCV, Face_pytorch, OpenFace and Insightface. Many of these software libraries are developed at universities or implement algorithms and neural network architectures presented in academic papers. They are free, and allow for a great detail of customisation, but require substantial programming skills to be implemented in a surveillance system. Moreover, when using such software, the algorithms run on one's own hardware which provides the developer with more control, but also requires more maintenance.

Proprietary facial recognition. There are three possible routes for the use of proprietary systems: There are "turnkey" systems sold by manufacturers such as Hikvision, Dahua, Anyvision or Briefcam. Those integrate the software and hardware, and as such can be directly deployed by the client. Algorithm developers such as Amazon AWS Rekognition (USA), NEC (Japan), NTechlab (Russia), Paravision (USA) allow to implement their algorithms and customise them to one's needs, and finally there are "cloud" API systems, a sub-set of the former category, where the algorithm is hosted in a datacentre and is accessed remotely (IPVM Team 2021b, 16). The latter type of technology bears important legal ramifications, as the data may travel outside of national or European jurisdictions. It should be noted that many of the proprietary products are based on similar algorithms and network architectures as their open-source counterparts (OpenCV, 2021). Contrary to the open-source software, it is generally unclear which datasets of images have been used to train the proprietary algorithms.

TECHNICAL LIMITS, PROBLEMS, AND CHALLENGES OF FACIAL RECOGNITION

Contrary to what can often be read in dystopian accounts of remote biometric identification technologies, these systems are neither "entirely inefficient", nor "all powerful". They are subjected to technical challenges and limitations, which should be considered in the broader analysis of their ethical, legal, and political implications.

Data capture challenges

Facial recognition's accuracy can easily be challenged by a certain number of factors in the capture of the data to be analysed, in particular when dealing with "non-cooperative" image capture. The resolution of the camera, and in particular the key variable of Pixels per Meter (minimum 300 PPM is generally required) is instrumental in ensuring that enough information is provided to the algorithm. Lighting conditions are similarly important. Although increasingly cameras add an infra-red channel to the RGB channels in order to recover detail in low-light conditions, inadequately illuminated faces will generate a high number of errors. Orientation of the face in relation to the camera is one more key factor to take into account, especially because a camera will rarely be mounted at face level (more likely overhead), and thus difficult angles will often result in partial representation of faces (Fernandez et al. 2020, 29). Vision can often be blocked by other factors, such as other individuals in large crowds, sunglasses, masks (in particular in times of COVID-19). Obstruction can be voluntary when individuals for example look down to avoid surveillance. Finally, not all systems have a liveness detection system, meaning that they can be tricked by a photograph of a face instead of a real face. (IPVM Team 2020, 12–13)

Dataset-related challenges

Datasets also face a number of technical challenges. For machine learning systems, small datasets will inadequately train the algorithms, simply because there are not enough different instances of the type of face or object that is supposed to be recognised. This is a challenge for gait recognition algorithms for example, for which there is a dearth of large datasets. Changes in features (such as hair, facial hair, beard, earrings) in the dataset can lead to a poorly trained algorithm. Datasets are often labelled with a specific purpose, and thus training an algorithm on a dataset that is not representative of the use-case can provide counter-productive results.

More problematically, a lack of diversity, in particular when it comes to ethnicity, age, or gender leads to bias in the algorithm. This issue has been at the core of the US-based discussion on the banning of Facial Recognition. Public databases such as VGGFace2 (based on faces from Google images) and MS-Celeb-1M42 (celebrity faces) are often used to train facial recognition algorithms yet are far from representative of everyday populations – this is called representation bias (Fernandez et al. 2020, 30). The main goal of the project Gender Shades led by Joy Buolamwini was both to show the lack of representativity of existing datasets and address the problem of the consequent discrepancy between the error rates related to light-skinned men and dark-skinned women (Fernandez et al. 2020, 30–31).

However, a representational dataset is not always a desirable dataset, because actual structural biases often do not match the values of society. Illustrative of this is that, when doing a Google image search for the term "CEO" it would originally return primarily photographs of white male people. While this was representative of the CEO population (and thus accurate), the results reinforce the vision of a world that does not align with progressive societal values (Suresh, 2019). Because of the gap between ideals of equality and actual societal structural inequalities, datasets can be either representative of an unequal society, or representative of desired equality – but never of both at the same time.

Datasets upon which the computer algorithm will later be able to distinguish particular entities or behaviour are built through vast amounts of human labour. For example,

the work that has gone into the image dataset ImageNet is equivalent to 19 years of working 24 hours a day, 7 days a week (Malevé, 2020). Nevertheless, quantity does not necessarily equal quality. Many of the categories with which images are annotated are ambiguous. Not in their dictionary definition per se, but when they enter the culture of the annotation workers. For example, the category of "ratatouille" contains images of various stews, salads and even a character of the eponymous Pixar movie. Similarly, the category "Parisian" contains images of Paris Hilton (Malevé, 2020). This ambiguity of categories does not only haunt ImageNet. The aforementioned COCO dataset contains images of a birdhouse in the shape of a bird, which is tagged as bird, or a bare pizza bottom which is tagged as pizza (Cochior and van de Ven, 2020). These examples show that even seemingly unambiguous concepts become fluid the moment they have to become strictly delineated in a dataset.

Another important issue with ethical and political repercussions is unethically collected data, as in the case of Clearview AI detailed above. When it comes to operational datasets, i.e., datasets used in the actual process of facial authentication and/or identification, we have seen that possible deployments include the use of cloud-based services (either for the processing or the storage of the sensitive information). This increases the risks of data breaches and attacks by hackers. (Fernandez et al. 2020, 34)

Algorithm-related challenges

Finally, there are issues related to the quality and performance of the algorithms and how to measure it. The National Institute of Standards and Technology is an agency of the US Department of Commerce. The NIST provides the possibility for vendors to test the efficacy of their algorithms on a standardised dataset, the "Ongoing Face Recognition Vendor Test (FRVT).

As an IPVM study shows, brands often use single-number scores obtained from NIST vendor tests (i.e., "our algorithm showed 98,6% accuracy".) (IPVM Team 2021b, 17). These scores are however obtained in very controlled conditions that do not match the real-world use of the algorithms. There are thus important discrepancies in this regard. Moreover, the accuracy score is not always representative of desirable behaviour of a model. Data scientists therefore distinguish precision and recall, to better account for cases where e.g., positive classification is rare, yet of high impact – for example when classifying individuals as high risk (Shung 2020, 202). These distinctions are often lost in the commercial language and in the public debate.

A final issue related to working with the existing algorithms is what is known as observer bias or confirmation bias. The output of an algorithm reinforces the (subconscious) biases that went into producing it. It can occur both when creating the dataset or when training and running the algorithms. For example, the software used for predictive policing in Chicago helped determine where to send police officers on patrol. "Because these predictions are likely to over represent areas that were already known to police, officers become increasingly likely to patrol these same areas and observe new criminal acts that confirm their prior beliefs regarding the distributions of criminal activity. The newly observed criminal acts that police document as a result of these targeted patrols then feed into the predictive policing algorithm on subsequent days, generating increasingly biased predictions. This creates a feedback loop where the model becomes increasingly confident that the locations most likely to experience further criminal activity are exactly the locations, they had previously believed to be high in crime." (Lum and Isaac, 2016). The example reveals that the different kinds of biases at play are hard to untangle, as

the observer bias coincides with a historical bias of over-policing. It requires a lot of work to recognise such confirmation biases in the automated operation of automated classification software. The "black box" dimension of their operation – and the only just emerging efforts to build explanatory AI – make it difficult to understand their categorisation process (Xie et al. 2020; Fernandez et al. 2020, 34)

CHAPTER 3

OVERVIEW OF DEPLOYMENTS IN EUROPE

OVERVIEW OF **DEPLOYMENTS IN EUROPE**

Key points

- Current deployments of RBI technologies within Europe are primarily experimental and localised. However, the technology coexists with a broad range of algorithmic processing of security images being carried out on a scale which ranges from the individual level to what could be classed as biometric mass surveillance. Distinguishing the various characteristics of these deployments is not only important to inform the public debate, but also helps to focus the discussion on the most problematic uses of the technologies.
- Image and sound-based security applications being used for authentication purposes do not currently pose a risk for biometric mass surveillance. However, it should be noted that an alteration to the legal framework could increase the risk of them being deployed for biometric mass surveillance especially as many of the databases being used contain millions of data subjects.
- In addition to authentication, image and sound-based security applications are being deployed for surveillance. Surveillance applications include the deployment of RBI in public spaces.
- Progress on two fronts makes the development of biometric mass surveillance more than a remote possibility. Firstly, the current creation and/or upgrading of biometric databases being used in civil and criminal registries. Secondly, the repeated piloting of live-feed systems connected to remote facial and biometric information search and recognition algorithms.

When looking at the map of actual deployments of image and sound-based security technologies in Europe, Remote Biometric Identification is, as this report is being written, so far mostly an experimental and localised application. It coexists alongside a broad range of algorithmic processing of security images in a spectrum that goes from individual, localised authentication systems to generalised law enforcement uses of authentication, to what can properly be defined as Biometric Mass Surveillance. Distinguishing the various characteristics of these deployments is not only important to inform the public debate, but it also helps focus the discussion on the most problematic uses of the technologies. It also highlights the risks of function creep: systems deployed for one use which is respectful of EU fundamental rights can in some cases very easily be upgraded to function as biometric mass surveillance.

The European map of image and sound-based security technologies can be divided into two broad categories: authentication applications and surveillance applications. Remote Biometric Identification is a sub-category of the latter.

AUTHENTICATION

A broad range of deployments, which we consider in this first section, is not aimed at surveillance, but at authentication (see section 2.3 in this report), namely making sure that the person in front of the security camera is who they say they are.

Live authentication

As in the cases of the use of Cisco systems powered FRT in two pilot projects in high schools of Nice (see section 8.1) and Marseille (France)[1], or as in the case of the Anderstorp Upper Secondary School in Skelleftea (Sweden)[2], the aim of these projects was to identify students who could have access to the premises. School-wide biometric databases were generated and populated with students' portraits. Gates were fitted with cameras connected to facial recognition technology and allowed access only to recognised students. Another documented use has been for the Home Quarantine App (Hungary), in which telephone cameras are used by authorities to verify the identity of the persons logged into the app (see also section 10.1).

In these deployments, people must submit themselves to the camera in order to be identified and gain access. While these techniques of identification pose important threats to the privacy of the concerned small groups of users (in both high school cases, DPAs banned the use of FRTs), and run the risk of false positives (unauthorised people recognised as authorised) or false negatives (authorised people not recognised as such) the risk of biometric mass surveillance strictly speaking is low to non-existent because of the nature of the acquisition of images and other sensor-based data.

However, other forms of live authentication tie in with surveillance practices, in particular various forms of blacklisting. With blacklisting the face of every passer-by is compared to a list of faces of individuals who have been rejected access to the premises. In such an instance, people do not have to be identified, as long as an image of their face is provided. This has been used in public places, for example in the case of the Korte Putstraat in the Dutch city of 's-Hertogenbosch: during the carnival festivities of 2019 two people were rejected access to the street after they were singled out by the system (Gotink, 2019). It is unclear how many false positives were generated during this period. Other cases of blacklisting

1 Both projects were shut down by the CNIL, the French DPA.

2 The project was shut down by the Swedish Authority for Privacy Protection (IMY)

can be found at, for example, access control at various football stadiums in Europe, see also section 3.3. In many cases of blacklisting, individuals do not enrol voluntarily.

Forensic authentication

Biometric systems for the purposes of authentication are also increasingly deployed for forensic applications among law-enforcement agencies in the European Union. The typical scenario for the use of such technologies is to match the photograph of a suspect (extracted, for example, from previous records or from CCTV footage) against an existing dataset of known individuals (e.g., a national biometric database, a driver's license database, etc.). (TELEFI, 2021). The development of these forensic authentication capabilities is particularly relevant to this study, because it entails making large databases ready for searches on the basis of biometric information.

To date, 11 out of 27 member states of the European Union are using facial recognition against biometric databases for forensic purposes: Austria (EDE)[3], Finland (KASTU)[4], France (TAJ)[5], Germany (INPOL)[6], Greece (Mugshot Database)[7], Hungary (Facial Image Registry)[8],

3 Criminal identification database, used by the Austrian Criminal Intelligence Service, managed by the Austrian Ministry of Interior.

4 The KASTU system interrogates two datasets: the Registered persons identifying features
database (RETU) and Aliens database. It is managed by the National Bureau of Investigation (NBI), and can be used by the Finnish Police, the Finnish Border Guard and the Finnish Customs.

5 Criminal case history database, managed by the French Ministry of Interior

6 Criminal case management system, managed by the German Federal Criminal Police Office (Bundeskriminalamt)

7 Managed by the Video and Image Laboratory of the Audiovisual Evidence of the Department of Photography and Modus Operandi of the Hellenic Police Forensic Science Division

8 The Facial Image registry is interrogated through a search engine developed by NEC, and accessible to the National Investigation Agency, the Criminal Courts, the National Protective Service, the Counter-Terrorism Centre, the Hungarian Prison Service, the Prosecution Service of Hungary, the Public Administration, the Special Service for National Security, the Intelligence Agencies, the Hungarian Police, the Hungarian Parliamentary Guard, Hungarian Ministry of Justice, Witness Protection Service, the National Directorate-General for Aliens Policing and Institution of the President of the Republic. As of September 2020 the NOVA. Mobile applications has been launched for police officers to identify people on the streets who do not have identity documents with them (TELEFI 2021, 86).

Figure 1. *EU Countries use of FRT for forensic applications*[1]

1 Source: TELEFI Report p.23. [[NOTE TO THE GREENS: A new map should be made to match report's design at a later stage in the publication process]]

Italy (AFIS)[9], Latvia (BDAS)[10], Lithuania (HDR)[11], Netherlands (CATCH)[12] and Slovenia (Record of Photographed Persons)[13] (TELEFI 2021).

Seven additional countries are expected to acquire such capabilities in the near future: Croatia (ABIS)[14], Czech Republic (CBIS)[15], Portugal (AFIS)[16] Romania (NBIS)[17], Spain (ABIS), Sweden (National Mugshot Database), Cyprus (ISIS Faces), Estonia (ABIS)[18] (TELEFI 2021).

When it comes to international institutions, Interpol (2020) has a facial recognition system (IFRS)[19], based on facial images received from more than 160 countries. Europol has two subunits which use the facial recognition search tool and database known as FACE: the European Counter Terrorism Center (ECTC) and the European Cybercrime Center (ECC). (TELEFI, 2021 149-153) (Europol 2020)

Only 9 countries in the EU so far have rejected or do not plan to implement FRT for forensic purposes: Belgium (see CHAPTER 6), Bulgaria, Denmark, Ireland, Luxembourg, Malta, Poland, Portugal, Slovakia.

9 Automated Fingerprint Identification System. The system, managed by the Italian ministry of interior can be interrogated via a software developed by the company Reco 3.26, a subsidiary of Parsec 3.26. Another software used is provided by the japanese company NEC.

10 Biometric Data Processing System (criminal data array), supported by database software from RIX Technologies, a search engine (MorphoTrust) provided by Idema and Safran Group managed by the Latvian ministry of interior.

11 Habitoscopic Data Register, managed by the Ministry of Interior (Lithuania)

12 Central Automatic TeChnology for Recognition of Persons, managed by the Centrum voor Biometrie,

13 The database uses VeriLook and Face Trace software from the Lithuanian company
Neurotechnology. It is managed by the Ministry of Interior (Slovenia).

14 Automated Biometric Identification System, searchable by the IntellQ software from the company IntellByte, managed by the Ministry of the Interior (Croatia).

15 Central Biometric Information System

16 National Biometric Identification System, managed by the Ministry of Interior (Romania)

17 Managed by the Photographic and Graphic Laboratory of Criminalistic Services, using search software by the company Unidas

18 Managed by the Estonian Ministry of Interior

19 Interpol Facial Recognition System

When it comes to databases, some countries limit the searches to criminal databases (Austria, Germany, France, Italy, Greece, Slovenia, Lithuania, UK), while other countries open the searches to civil databases (Finland, Netherlands, Latvia, Hungary).

This means that the person categories can vary substantially. In the case of criminal databases it can range from suspects and convicts, to asylum seekers, aliens, unidentified persons, immigrants, visa applicants. When civil databases are used as well, such as in Hungary, the database contains a broad range of "individuals of known identity from various document/civil proceedings" (TELEFI 2021, appendix 3).

Finally, the database sizes, in comparison to the authentication databases mentioned in the previous section, are of a different magnitude. The databases of school students in France and Sweden, mentioned in the previous section contains a few hundred entries. National databases can contain instead several millions. Criminal databases such as Germany's INPOL contains 6,2 million individuals, France's TAJ 21 million individuals and Italy's AFIS 9 million individuals. Civil databases, such as Hungary's Facial Image Registry contain 30 million templates (TELEFI, 2021 appendix 3).

Authentication has also been deployed as part of integrated "safe city" solutions, such as the NEC Technology Bio-IDiom system in Lisbon and London, deployed for forensic investigation purposes. For this specific product, authentication can occur via facial recognition, as well as other biometric authentication techniques such as ear acoustics, iris, voice, fingerprint, and finger vein recognition. We currently do not have public information on the use of Bio-IDiom in Lisbon nor in London. On NEC's Website (2021) however, Bio-IDiom is advertised as a "multimodal" identification system,

that has been used for example by the Los Angeles County Sheriff's Department (LASD) for criminal investigations. The system "combines multiple biometric technologies including fingerprint, palm print, face, and iris recognition" and works "based on the few clues left behind at crime scenes. In Los Angeles, "this system is also connected to the databases of federal and state law enforcement agencies such as the California Department of Justice and FBI, making it the world's largest-scale service-based biometrics system for criminal investigation". We don't know if that is the case in Portugal and in the UK deployments.

Case study: INPOL (Germany)

In order to give a concrete example of the forensic use of biometric technology, we can take the German case. Germany has been using automated facial recognition technologies to identify criminal activity since 2008 using a central criminal information system called INPOL (Informationssystem Polizei), maintained by the Bundeskriminalamt (BKA), which is the federal criminal police office. INPOL uses Oracle Software and includes the following information: name, aliases, date and place of birth, nationality, fingerprints, mugshots, appearance, information about criminal histories such as prison sentences or violence of an individual, and DNA information. However, DNA information is not automatically recorded (TELEFI 2021).

The INPOL database includes facial images of suspects, arrestees, missing persons, and convicted individuals. For the purpose of facial recognition, anatomical features of a person's face or head as seen on video surveillance or images are used as a material to match with data in INPOL. The facial recognition system compares templates and lists all the matches ordered by degree of accordance. The BKA has specific personnel visually analysing the system's choices and providing an assessment, defining the probability of identifying a person. This assessment can be used in a court of law if necessary (Bundeskriminalamt, n.d.). Searches in the database are conducted by using Cognitec Face VACS software (TELEFI 2021).

As of March 2020, INPOL consists of 5,8 million images of about 3,6 million individuals. All police stations in Germany have access to this database. The BKA saves biometric data and can be used by other ministries as well, for instance, to identify asylum seekers. Furthermore, the data is shared in the context of the Prüm cooperation on an international level (mostly fingerprints and DNA patterns). Furthermore, the BKA saves DNA analysis data as part of INPOL, accessible for all police stations in Germany. That database contains 1,2 million data sets (Bundeskriminalamt, n.d.). Other recorded facial images, for instance, driver's licenses or passports, are not included in the search, and the database is mainly used for police work (TELEFI 2021).

A blurred boundary between authentication and surveillance

In principle, because of the strict legal framework to which law enforcement agencies are submitted, forensic biometric identification should not present a risk of biometric mass surveillance. The acquisition of images and the subsequent one-to-one searches are carried out as part of judicial investigations when a legal threshold of suspicion is met. The operation of the system by specialised forensic departments should follow the procedural limits set by the judicial process.

Function creep is however particularly concerning. If the legal framework is altered to allow the acquisition of live video, and if live searches on these are legally authorised against existing criminal and civil databases, then from a technical perspective it can be argu-

ed that there is potentially a risk of biometric mass surveillance. The main risk here being that the individuals whose identities are searched or tagged are not selected as a result of a judicial investigation, but indiscriminately. The system in place would then allow for search of these individuals against huge databases. In other words, by creating new biometric databases or upgrading existing databases to be FRT-readable, and developing or acquiring algorithmic capabilities to search them, law enforcement agencies across Europe are building an infrastructure which is technically capable of "switching" easily to a mode of operation akin to biometric mass surveillance.

SURVEILLANCE

A second broad use of image and audio-based security technologies is for surveillance purposes. Here again, it is important, we suggest, to distinguish between two broad categories.

Smart surveillance features

A first range of deployments of "smart" systems correspond to what can broadly be defined as "smart surveillance" yet do not collect or process biometric information per se[20]. Smart systems can be used ex-post, to assist CCTV camera operators in processing large amounts of recorded information, or can guide their attention when they have to monitor a large number of live video feeds simultaneously. Smart surveillance uses the following features:

- Anomaly detection. In Toulouse (France), the City Council commissioned IBM to connect 30 video surveillance cameras to software able to "assist human decisions" by raising alerts when "abnormal events are detected." (Technopolice 2021) The request was justified by the "difficulties of processing the images generated daily by the 350 cameras and kept for 30 days (more than 10,000 images per second)". The objective, according to the digital direction is "to optimise and structure the supervision of video surveillance operators by generating alerts through a system of intelligent analysis that facilitates the identification of anomalies detected, whether: movements of crowds, isolated luggage, crossing virtual barriers north of the Garonne, precipitous movement, research of shapes and colour. All these detections are done in real time or delayed (Technopolice 2021). In other words, the anomaly detection is a way to operationalise the numerical output of various computer vision based recognition systems. Similar systems are used in the Smart video surveillance deployment in Valenciennes (France) or in the Urban Surveillance Centre (Marseille).

- Object Detection. In Amsterdam, around the Johan Cruijff ArenA (Stadium), the city has been experimenting with a Digitale Perimeter (digital perimeter) surveillance system. In addition to the usual features of facial recognition, and crowd monitorining, the system includes the possibility of automatically detecting specific objects such as weapons, fireworks or drones. Similar features are found in Inwebit's Smart Security Platform (SSP) in Poland.

- Feature search. In Marbella (Spain), Avigilon deployed a smart camera system aimed at providing "smart" functionalities without biometric data. Since regional law bans facial and biometric identification without consent, the software uses "appearance search". "Appearance search" provides estimates for "unique facial traits, the colour of a person's clothes, age, shape, gender and hair colour". This information is not considered biometric. The individual's features can be used to search for suspects fitting a particular profile. Similar technology has been deployed in Kortrijk

20 As detailed in CHAPTER 4. However, that does not mean that it is not subjected to similar legal frameworks.

(Belgium), which provides search parameters for people, vehicles and animals (Verbeke 2019). During the Covid-19 pandemic, several initiatives emerged to automatically detect whether the mask mandates were observed by the public, such as in the aborted face mask recognition project in Châtelet-Les Halles developed by the company Datakalab.

- Video summary. Some companies, such as Briefcam and their product Briefcam Review, offer a related product, which promises to shorten the analysis of long hours of CCTV footage, by identifying specific topics of interest (children, women, lighting changes) and making the footage searchable. The product combines face recognition, license plate recognition, and more mundane video analysis features such as the possibility to overlay selected scenes, thus highlighting recurrent points of activity in the image. Briefcam is deployed in several cities across Europe, including Vannes, Roubaix (in partnership with Eiffage, managed by the City of Roubaix and the Métropole Européenne de Lille) and Moirans in France (with equipment provided by Nomadys).

- Object detection and object tracking. As outlined in chapter 2, object detection is often the first step in the various digital detection applications for images. An 'object' here can mean anything the computer is conditioned to search for: a suitcase, a vehicle, but also a person; while some products further process the detected object to estimate particular features, such as the colour of a vehicle, the age of a person. However, on some occasions — often to address concerns over privacy — only the position of the object on the image is stored. This is for example the case with the test of the One-and-a-half-meter monitor in Amsterdam (Netherlands), Intemo's people counting system in Nijmegen (Netherlands), the ViSense social distancing monitor at MINDBase, a testing location of the Dutch Defence Equipment Organization; the KICK project in Brugge, Kortrijk, Ieper, Roeselare and Oostende (Belgium), the ViSense project in Mechelen (Belgium) or the Eco-counter tracking cameras pilot project in Lannion (France).

- Movement recognition. Avigilon's software that is deployed in Marbella (Spain) also detects unusual movement. "To avoid graffiti, we can calculate the time someone takes to pass a shop window, "explained Javier Martín, local chief of police in Marbella to the Spanish newspaper El País. "If it takes them more than 10 seconds, the camera is activated to see if they are graffitiing. So far, it hasn't been activated." (Colomé 2019) Similar movement recognition technology is used in, the ViSense deployment at the Olympic Park London (UK) and the security camera system in Mechelen-Willebroek (Belgium). It should be noted that movement recognition can be done in two ways: where projects such as the Data-lab Burglary-free Neighbourhood in Rotterdam (Netherlands)[21] are only based on the tracking of trajectories of people through an image (see also 'Object detection'), cases such as the Living Lab Stratumseind[22] in Eindhoven (Netherlands) also process the movements and gestures of individuals in order to estimate their behaviour.

Audio recognition

- In addition to image (video) based products, some deployments use audio recognition to complement the decision-making process, for example used in the Serenecity (a branch of Verney-Carron) Project in Saint-Etienne

21 Developed as a partnership between the Dutch Ministry of Justice & Security, the Dutch Institute for Technology Safety and Security (DITSS), the Rotterdam Municipality, the Interpolis, the Dutch Police, the ViNotion, the Avans Hogeschool, the Munisense, the Sustainder, the Twente University, the Max Planck Institute for the Study of Crime, the Security and Law and The Network Institute (Vrij University).

22 Developed in partnership between the Dutch Institute for Technology Safety and Security (DITSS), Atos, the Municipality of Eindhoven, Tilburg University, Eindhoven University of Technology, Intel, Sorama, and Axis Communications; it uses search software from Oddity.ai (a spinout of Utrecht University) and ViNotion.

(France), the Smart CCTV deployment in public transportation in Rouen (France) or the Smart CCTV system in Strasbourg (France). The project piloted in Saint-Etienne for example, worked by placing "audio capture devices" - the term microphone was avoided- in strategic parts of the city. Sounds qualified by an anomaly detection algorithm as suspicious would then alert operators in the Urban Supervision Center, prompting further investigation via CCTV or deployment of the necessary services (healthcare or police for example) (France 3 Auvergne-Rhône-Alpes 2019.)

Emotion recognition

- Emotion recognition is a rare occurrence. We found evidence of its deployment only in a pilot project in Nice (see section 8.1) and in the Citybeacon project in Eindhoven, but even then, the project was never actually tested. The original idea proposed by the company Two-I was "a "real-time emotional mapping" capable of highlighting "potentially problematic or even dangerous situations". "A dynamic deployment of security guards in an area where tension and stress are felt, is often a simple way to avoid any overflow," also argues Two-I, whose "Security" software would be able to decipher some 10,000 faces per second. (Binacchi 2019)

Gait recognition

Gait recognition is currently not deployed in Europe. To our knowledge, only one company, Watrix (a company based in China), has commercialised gait recognition, but only in China (Segal 2020, 2).

Integrated solutions

Smart cities

While some cities or companies decide to implement some of the functionalities with their existing or updated CCTV systems, several chose to centralise several of these "smart" functions in integrated systems often referred to as "safe city" solutions. These solutions do not necessarily process biometric information. This is the case for example for the deployments in TIM's, Insula and Venis' Safe City Platform in Venice (Italy), Huawei's Safe City in Valenciennes (France), Dahua's integrated solution in Brienon-sur-Armançon (France), Thalès' Safe City in La Défense and Nice (France), Engie Inéo's and SNEF's integrated solution in Marseille (France), the Center of Urban Supervision in Roubaix (France), AI Mars (Madrid, in development)[23] or NEC's platform in Lisbon and London.

The way "Smart/Safe City" solutions work is well exemplified by the "Control room" deployed in Venice, connected to an urban surveillance network. The system is composed of a central command and control room which aggregates cloud computing systems, together with smart cameras, artificial intelligence systems, antennas and hundreds of sensors distributed on a widespread network. The idea is to monitor what happens in the lagoon city in real time. The scope of the abilities of the centre is wide-ranging. It promises to: manage events and incoming tourist flows, something particularly relevant to a city which aims to implement a visiting fee for tourists; predict and manage weather events in advance, such as the shifting of tides and high water, by defining alternative routes for transit in the city; indicating to the population in real time the routes to avoid traffic and better manage mobility for time optimisation; improve the management of public safety allowing city agents to intervene in a more timely manner; control and manage water and road traffic, also for sanctioning purposes, through specific video-analysis systems; control the status of parking lots; monitor the environmental and territorial

23 Developed by Retevision, Instituto Tecnológico de Castilla y León (ITCL), Centro para el Desarrollo Tecnológico Industrial, Cellnex, Herta Security, Sngular, Emergya, SHS, Televés, Universidad de Granada, Universidad Politecnica de Madrid, Universidad Carlos III.

situation; collect, process data and information that allow for the creation of forecasting models and the allocation of resources more efficiently and effectively; bring to life a physical "Smart Control Room" where law enforcement officers train and learn how to read data as well. (LUMI 2020)

Smartphone apps

Integrated solutions can entail smartphone apps, used to connect citizens with the control and command centres. This is for example the case in Nice with the (failed) Reporty App project (See Chapter 5), the Dragonfly project (Hungary) (See chapter 10) and was part of the original plan of Marseille's Safe City project.

Crowd management

Integrated solutions are generally comprised of a set of crowd management features, such as in the case of the systems in Valenciennes and Marseille (France), Mannheim (Germany), Venice (Italy), Amsterdam, Eindhoven and Den Bosch with the pilot in the Korte Putstraat (using software by CrowdWatch, Netherlands). Such crowd management software generally does not recognise individuals, but rather estimates the number of people on (a part of) the video frame. Sudden movements of groups or changes in density are then flagged for attention of the security operator (Nishiyama 2018).

REMOTE BIOMETRIC IDENTIFICATION

While all the deployments described above are variants of security applications of algorithmically processed images and sound, the number of deployments which match the narrow definition of Remote Biometric Identification (RBI), namely the use of live camera feeds processed through search algorithms against pre-existing databases, is relatively small. They are often presented as "pilots", limited in time and often quickly interrupted for legal reasons.

Deployment of RBI in public spaces

Here are the documented cases of RBI in public spaces we could find through our research:

- Live Facial Recognition pilot project in Brussels International Airport / Zaventem (Belgium, see detailed case study, CHAPTER 6)
- Live Facial Recognition in Budapest (Hungary, see detailed case study, CHAPTER 10)
- Live Facial Recognition pilot project during the Carnival in Nice (France, see detailed case study, CHAPTER 8)
- Live Facial Recognition Pilot Project Südkreuz Berlin (Germany, see detailed case study, CHAPTER 9)

As most of these cases are extensively discussed in the following chapters, we do not comment further on them here.

Additional cases are the Live Facial Recognition pilot during Carnival 2019 in 's-Hertogenbosch's Korte Putstraat (the Netherlands) and the pilot of Live Facial Recognition in the city of Como[24], recently struck down by the Italian DPA (Garante per la Privacy). The deployment of facial recognition in Estacion Sur in Madrid (Spain) is also live.

Deployment of RBI in commercial spaces

The number of deployments of live facial recognition systems in commercial spaces hosting the public is much higher, but because of its commercial nature, difficult to document and trace. Our research found the following instances:

- Live Facial Recognition project, Brøndby IF Football stadium (Denmark)
- Live Facial Recognition Pilot in Metz Stadium (France)
- Live Facial Recognition in Ifema (Spain)
- Live Facial Recognition in Mercadona or Mallorca, Zaragoza, Valencia (Spain)

24 Using the software SARI by the company Parsec 3.26, developed in partnership with Telecom Italia

The systems operate more or less in the same way as RBI in public spaces, or as forensic authentication systems if they were connected to live cameras. In the Brøndby IF Football stadium deployment for example, developed in partnership with Panasonic and the National University of Singapore, the football fans who want to access the game have to pass through a gate equipped with a camera, connected to a facial recognition algorithm. The stadium administration has constituted a database of unwanted individuals and if the software matches one of the incoming fans with a record in the database, it flags it to the system (Overgaard 2019).

There is however little to no information of the uses of these technologies in commercial spaces, as there is no requirement to publicise the various components of these systems. The case studies of this report thus focus mostly on the deployment of RBI in public spaces. More research, and more transparency would however be welcome in order to understand the data gathering practices and the impact of these deployments.

CONCLUSION

To conclude the overview of the deployment of "smart" security applications in Europe, "actually existing" Remote Biometric Identification deployments are a rare occurrence, but they are part of a much broader infrastructure of automated biometric authentication and smart surveillance that are increasingly maturing. The existence of this broader technical infrastructure means that while all the components necessary for biometric mass surveillance are not yet assembled, if given the legal authorisation, Remote Biometric Identification could potentially be deployed at a scale that could enact Biometric Mass Surveillance.

That this is more than a remote possibility as evidenced by progress in two directions that are necessary pre-conditions for Biometric Mass Surveillance: 1) The creation of large, new biometric databases, or the upgrading of existing databases, both of civil and criminal registries, so that they can be searched by FRT and other biometric recognition algorithms on a broad scale by country-wide agencies. 2) The repeated piloting and experimentation of live-feed systems connected to remote facial and biometric information search and recognition algorithms. The evolution of these two developments (database integration and live deployment pilots), while carried out in general by different categories of actors (national law enforcement for the former, municipal police and city authorities for the latter) should however be analysed together, and given a permissive legislative framework, they demonstrate the plausible characteristics of potential technical systems of Biometric Mass Surveillance. In the following chapter, we explore the current legal framework that limits the existing technological developments and explore the growing jurisprudence on the matter.

CHAPTER 4

LEGAL BASES

LEGAL BASES

Key points

- The use of biometric tools for law enforcement purposes in public spaces raises a key issue of the legal permissibility in relation to the collection, retention and processing of data when considering the individual's fundamental rights to privacy and personal data protection. When viewed through this lens, RBI technologies could have a grave impact on the exercise of a range of fundamental rights.
- The deployment of biometric surveillance in public spaces must be subject to strict scrutiny in order to avoid circumstances which could lead to mass surveillance. This includes targeted surveillance which has the potential for indiscriminate collection of data on any persons present in the surveilled location, not only that of the target data subject.
- The normative legal framework for conducting biometric surveillance in public spaces can be found in the EU secondary legislation on data protection (GDPR and LED). The use of biometric data under this framework must be reviewed in light of the protection offered by fundamental rights.
- The European Commission's April 2021 proposal on the Regulation for the Artificial Intelligence Act aims to harmonise regulatory rules for Member States on AI-based systems. The Proposed Regulation lays out rules focussed on three categories of risks (unacceptable, high, and low/ minimal risk) and anticipates covering the use of RBI systems. It also aims to compliment the rules and obligations set out in the GDPR and LED.

The deployment of remote biometric identification in public spaces might have grave effects on the exercise of a range of fundamental rights of individuals (FRA 2019) such as the right to peaceful assembly and association (UNHRC 2019, para. 57) and the rights to liberty and security. Because the use of biometric tools for law enforcement purposes in public spaces involves collection, retention and processing of biometric data, a key issue on their legal permissibility is raised in relation to the obligations under the fundamental rights to privacy and personal data protection. This section thus will consider remote biometric identification against the protection offered by EU fundamental rights framework for the rights to privacy and personal data protection as well as by EU data protection legislation.

EU FUNDAMENTAL RIGHTS FRAMEWORK FOR THE RIGHT TO PRIVACY AND THE RIGHT TO PROTECTION OF PERSONAL DATA

The scope of the fundamental right to protection for RBI

Article 7 of the EU Charter of Fundamental Rights (Charter) sets out national and EU legislators' obligations on guaranteeing the right to private life, family life, and communications of individuals (the right to privacy) under EU law. The right to privacy can also be found in Article 8 of the European Convention on Human Rights (ECHR), the scope of which has evolved over the years to cover issues relating to the processing of personal data. Because Article 7 of the Charter mirrors closely Article 8 ECHR, its scope must be interpreted in line with the latter and its interpretation by the European Court of Human Rights (ECtHR) pursuant to Article 52(3) of the Charter. The Charter enshrines a separate right to protection of personal data in its Article 8, which is "distinct from Article 7 of the Charter" (C-203/15, Tele2, para. 129).

Biometric surveillance tools interfere with the fundamental rights to privacy and personal data protection as enshrined in each of these legal sources because they collect, retain, process and use personal data, including an intrinsically special category of biometric data, which is - as discussed below, personal data relating to the physical, physiological or behavioural characteristics of an individual that allows their unique identification (see section 4.2.1). Notably, it may not be just the physical biometric data such as fingerprints (S and Marper v UK; C-291/12 , Schwarz) or facial images (Gaughran v UK) that benefits from the rights to privacy and personal data protection as enshrined in the ECHR and EU law. For example, the ECtHR has adopted an expansive approach in terms of recognising the protective scope of Article 8 ECHR (S and Marper v UK, para 67), which would afford protection to different categories of biometric data including behavioural biometric data such as one's way of movement or voice (Venier and Mordini, 2010).

Privacy and data protection in public space and the risk of mass surveillance

The use of a wide range of biometric data discussed above engages with the individuals' right to privacy and data protection even if they are captured and used in public spaces while individuals enjoy public life. The case law of the ECtHR (PG and JH v UK; Peck v UK) and the Court of Justice of the European Union (CJEU) (Opinion 1/15) shows that they have afforded privacy protection to information that is not inherently private. In fact, performing biometric surveillance in public spaces is inherently intrusive and amounts to mass surveillance, which in this context can simply be characterised as monitoring, tracking, or processing of personal data of individuals indiscriminately and in a generalised manner without a prior criminal suspicion (FRA 2018). Biometric surveillance in public spaces relies

on generalised and indiscriminate collection, retention, use and sharing of biometric data of individuals. This is the case even if the intended purpose of the biometric surveillance is targeted, because in order to identify people on the watchlist in a crowd, every person in that particular space must be analysed and compared with the watchlist (Houwing 2020).

The grave consequences of this type of indiscriminate and generalised collection of personal data on fundamental rights of individuals can be found across the case law of the ECtHR and the CJEU. The ECtHR has repeatedly warned that covert surveillance tools must not be used to undermine or even destroy democracy on the grounds of defending it (Klass and others v Germany, para 49). Particularly in considering the lawfulness of collection of biometric data, the ECtHR recognised in S and Marper v UK that the use of biometric data that would allow identification of an individual and would carry the potential to deduce personal data that is classified as sensitive data such as ethnic origin would make the people concerned fundamentally vulnerable to stigmatisation and discrimination (paras 122-126). Because of the heightened level of protection afforded to it, the ECtHR found that generalised and indiscriminate collection and retention of biometric data did not comply with the ECHR requirements as it amounted to disproportionate interference with the right to privacy and thus constitute a violation of Article 8 ECHR.

The CJEU considered in Digital Rights Ireland (Joined Cases C293/12 and C594/12, para 37) as well as Tele2 (C-203/15, para 100) that EU law precluded the mass retention of traffic and location data for law enforcement purposes, and only allowed for targeted retention of said data. The deployment of biometric surveillance in public spaces thus must be subject to strict scrutiny and in light of the case law of both courts, the EU fundamental rights law as well as the ECHR preclude the deployment of biometric surveillance that leads to mass surveillance for law enforcement purposes in public spaces.

The ambiguities of "targeted" biometric surveillance

Targeted biometric surveillance may still be lawful provided that it is justified under Article 52(1) of the Charter in light of the ECHR requirements for the Convention rights that are mirrored in the Charter. This type of surveillance is distinguishable from mass surveillance as it is directed towards a person or group of persons based on a prior suspicion on their involvement with criminal activities. Recently in its La Quadrature du net and others decision, the CJEU added a geographical criterion as a satisfactory limitation for a targeted retention of traffic and location data (para 149). However, in the context of conducting biometric surveillance in public spaces, this might not be a limitation as such. As mentioned above, by its nature this type of surveillance would amount to mass surveillance since it would indiscriminately monitor and analyse everyone in that space to detect people on the watchlist. Accordingly, using biometric surveillance in a specific area (e.g., concert venues, football stadiums, public rallies) for law enforcement purposes might be considered as expansive and intrusive to an extent that it would constitute disproportionate interference with the rights to privacy and personal data protection.

Conditions for "targeted" biometric surveillance

Even where biometric surveillance is performed in a targeted way, its lawfulness would turn on the legitimate aim for which it is conducted and an assessment on its proportionality in light of that aim. A key issue here is that conducting targeted biometric surveillance in public spaces would constitute a serious inter-

ference with the rights to privacy and personal data protection because of the special character of biometric data that makes a person unique and identifiable and potentially carries the risk to reveal sensitive data. Thus, it should be conducted for an aim that is proportionate to the level of intrusiveness caused by it (by analogy C-203/15, Tele2, para 102). In essence, this means that targeted biometric surveillance is only allowed if it is strictly necessary for the purpose of fighting against terrorism or serious crime (by analogy C-203/15, Tele2). There must be appropriate safeguards protecting people concerned from possible abusive uses of biometric surveillance. Moreover, there must be effective legal remedies available to people regarding the use of biometric surveillance. Authorisations for targeted biometric surveillance must be subject to effective review by a court or an independence administrative body who has the power to issue legally binding decisions to verify that a situation justifying the recourse to the measure exists and the conditions and safeguards are observed (C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, para 179).

A fundamental rights assessment of conducting targeted biometric surveillance in public spaces must be carried out in each stage of the data lifecycle, including when the data is processed in near real-time before collection. Especially where the personal data captured in the public sphere in real-time involves the use of data that the individual may not foresee (Uzun v Germany, para 45), that real-time automated processing would trigger an Article 8 protection. Similarly in the context of the right to personal data protection, the CJEU found in La Quadrature du Net and others (C-511/18, C-512/18 and C-520/18) that the automated analysis of personal data amounted to an interference with the right to protection of personal data as set out in Article 8 of the Charter, even though it did not initially involve the collection of the data (para 170). Based on the case law of both courts, the automated analysis of biometric data in and of itself amounts to an interference with the right to privacy and personal data protection and must meet the fundamental rights requirements to be lawful. Accordingly, it must be subject to review by a court or an independent administrative body, and the pre-established tools or models used in the automated analysis must meet certain qualities (e.g., they must non-discriminatory, specific, and reliable; any positive result must be subject to manual and individual re-examination) (C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, paras 180-182).

EU SECONDARY LAW: GDPR & LED

The normative legal framework for conducting biometric surveillance in public spaces can be found in the EU secondary legislation on data protection. The use of biometric data under this framework must be reviewed in light of the protection offered by fundamental rights (Section a).

"Biometric data" in GDPR & LED

The General Data Protection Regulations (GDPR) provides the rules relating to the processing of personal data for all purposes except where the processing is carried out for the prevention, investigation, detection, or prosecution of criminal offences including the safeguarding against and the prevention of threats to public safety pursuant to its Article 2(2)(d). The Law Enforcement Directive (LED) complements the GDPR in this area as it applies specifically to the processing of personal data by competent authorities for the prevention, investigation, detection, or prosecution of criminal offences including the safeguarding against and the prevention of threats to public safety pursuant to its Article 1.

Both legislations provide a specific framework for the processing of special categories of

data (formerly known as "sensitive data") – including biometric data, which is defined 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 or "dactyloscopic data" under Article 4(14) of the GDPR and Article 3(13) of the LED. The definition thus recognises expanding categories of biometric data that can capture and measure human characteristics as it covers physical and physiological as well as behavioural biometric data. Notably, biometric data is granted a higher protection than non-sensitive personal data irrespective of the fact that they may not reveal sensitive information such as racial or ethnic origin, health, or sexual orientation.

Distinguishing personal data and biometric data

There are two elements that need to be sought for the personal data to constitute biometric data and for their processing to be subject to the specific limitations imposed by the GDPR and the LED.

-"Specific technical process". Neither legislation defines the concept "specific technical process" but it should be understood as a special type of processing that captures the digital representation of biometric characteristics (e.g., facial images, fingerprints, voice) (Kindt 2013, 43; Jasserand 2016, 303). On this point, the European Data Protection Board (EDPB, 2019) notes that biometric data are the result of measurement of physical, physiological, or behavioural characteristics of individuals and thus the result of this special type of processing is captured by the concept of biometric data. For example, the image of the person captured by video surveillance is personal data, but it would be classified as biometric data once it is subjected to a specific type of processing to deduce the characteristics of that person (Recital 51, GDPR).

- "Unique identification of an individual". Compared to the definition of personal data, it is unclear whether the element of identification for the purpose of defining biometric data requires a higher threshold (Jasserand 2013, 305-306). Both legislations define personal data broadly, as "any information relating to an identified or identifiable individual". It has been confirmed both by the former Article 29 Data Protection Working Party (2007) and the CJEU (C-582/14, Breyer) that the personal data is broadly defined to capture the concept of "identifiability" whereby a person could be identifiable combined with other information available (including the information retained by someone other than the data controller) even if the person is not prima facie identified (paras 39-49).

The element of identification in the definition of biometric data on the other hand may suggest that said data must relate to an identified individual. The fact that the person could be identifiable through possible means would not be sufficient for the personal data to be classified as biometric data (Jasserand 2013, 306). The EDPB (2019) supports this view as it notes that if video surveillance system is set to detect the physical characteristics of individuals to classify them as opposed to uniquely identify them, this processing would not be subject to the framework reserved for the processing of sensitive data. Nevertheless, the data captured might still amount to personal data irrespective of the fact that they are not subject to any special type of processing.

Sensitive (biometric) data processing conditions

Both the GDPR and the LED impose a special framework for the processing of sensitive data including biometric data as opposed to

non-sensitive personal data. In essence, they impose limitations on the processing of sensitive data by setting out exceptional conditions for which the data may be processed. The following section considers the conditions under the LED on the processing of biometric data in order to set out the regulatory obligations relevant to implementing biometric surveillance in public spaces for law enforcement purposes. The conditions for biometric data processing under the GDPR are excluded from the scope of this report because it does not apply to processing activities for law enforcement purposes.

Conditions for the processing of biometric data under the LED

The LED imposes limitations to the processing of biometric data for the purpose of uniquely identifying an individual. Pursuant to its Article 10, competent authorities may process biometric data where strictly necessary (which requires a stringent balancing analysis between the data processing and its purpose) and is subject to appropriate safeguards for three purposes:

where authorised by EU or Member States' national law to protect the vital interests of the data subject or another person where the data is manifestly made public by the data subject

Clearly, the most relevant lawful ground for conducting biometric surveillance under the LED is where the processing is authorised by EU or a Member States' national law because, for example, processing for the protection of vital interests is limited to scenarios where the data subject or another person is physically or legally incapable of giving consent, or where there is a humanitarian emergency.

Accordingly, the EU legislator or Member States may adopt a law on conducting biometric surveillance for law enforcement purposes, but it would be subject to the EU fundamental rights requirements and would be unlawful if it affects the essence of the fundamental rights or if it amounts to a disproportionate interference.

Automated decision-making under the LED

Member States have discretion to use biometric data in automated decision-making processes subject to certain conditions. According to Article 11(1) of the LED, automated decision-making is prohibited unless authorised by EU or Member States law, which "provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller". Particularly when that automated decision-making uses sensitive data including biometric data, the law must provide suitable measures taking into account the nature of that data (Article 11(2), the LED). However, there are restrictions on conducting biometric surveillance where it involves a profiling process, which is considered a form of automated decision-making process that evaluates the person's personal aspects pursuant to Article 3(4) of the LED. Article 11(3) of the LED provides an unconditional prohibition against conducting profiling that has a discriminatory effect on individuals based on their sensitive data (including biometric data) under EU law. It is thus important to review the existence of the discriminatory effect of biometric surveillance that involves profiling because according to the LED, national law must introduce a human intervention in this context.

Competent authority under the LED

Another issue with the deployment of biometric surveillance in public spaces for law enforcement purpose is that the LED only applies to cases where the data controller is the "competent authority" to process the data for the relevant purpose. Determining what competent authority means is thus important to un-

derstand for example whether, and if so when, a private actor may qualify as an authority as such. Pursuant to Article 3(7)(a) and (b) of the LED, competent authority is a public authority that is entrusted with the power to prevent, investigate, detect, or prosecute criminal offences, and is any other entity or body that exercises public authority and public powers for the relevant purpose based on national law. It remains open to discussion whether the latter reference indicates that a private actor must be entrusted by law to process personal data (including biometric data) to process personal data for law enforcement purposes under the LED (Garstka 2018).

EU SOFT LAW: CONVENTION 108+

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal data (Convention 108), which is one of the bases for EU data protection legislation, was updated in 2018. The modernised Convention 108, which is known as Convention 108+, prohibits the processing of sensitive data (subject to certain conditions), in a similar, albeit arguably more modest (Greenleaf 2016), way to the GDPR. It lays out similar data subject rights, including the right not to be subjected to a sole automated decision-making process (Article 9). Although Article 11 of Convention 108+ permits the Signatory Parties to derogate from certain rules and obligations including the purpose limitation (Article 5(4)) and the duty to inform about data breaches (Article 7(2)) based on national security interests, it expressly requires the need to establish independent and effective review and supervision of data processing activities in a national security context (Article 11(3)). While Convention 108+ has yet to be ratified by all EU Member States, it provides a strong standpoint for establishing an oversight mechanism for surveillance measures.

CHAPTER 5

MAIN POLITICAL ISSUES AND DEBATES

MAIN POLITICAL ISSUES AND DEBATES

Key points

- Four main positions on RBI systems have emerged among political actors as a result of both technical developments in the field and early legislative activity of EU institutions: 1) active promotion 2) support with safeguards; 3) moratorium and 4) outright ban.
- Developments in the field of AI for governance, securitisation and law enforcement are widely encouraged and financed at an EU level through funding bodies such as the Digital Europe programme, the Connecting Europe Facility 2 and Horizon Europe.
- Those who are in favour of support with safeguards argue that the deployment of RBI technologies should be strictly monitored because of the potential risks they pose, including the potential danger of FRT, for example, to contribute to the further criminalisation or stigmatisation of groups of people who already face discrimination.
- The European Parliament passed a resolution on artificial intelligence in January 2020 in which they invite the Commission "to assess the consequences of a moratorium on the use of facial recognition systems". If deemed necessary, such a moratorium could impact some existing uses of FRT including its deployment in public spaces by public authorities.
- A number of EU and national NGOs have called for an outright ban on the use of RBI with some arguing that the mass processing of biometric data from public spaces creates a serious risk of mass surveillance that infringes on fundamental rights.
- The European Commission's legislative proposal for an Artificial Intelligence Act (EC 2021b) is both a proposal for a regulatory framework on AI and a revised coordinated plan to support innovation. One feature of the act is the establishment of risk-dependent restrictions which would apply to the various uses of AI systems

THE EMERGENCE OF REMOTE BIOMETRIC IDENTIFICATION AS A POLICY ISSUE

The technological developments in the field of remote biometric identification and the early legislative activity of EU institutions have progressively consolidated four main positions in relation to Remote Biometric Identification: 1) active promotion 2) support with safeguards; 3) moratorium and 4) outright ban. In this section we visit each of these positions and detail the logic of the arguments upon which they are based.

As detailed in the introduction, so far, the European Commission and the European Council have generally supported the development of Remote Biometric Identification. In the White Paper on AI he European Commission (2020b) proposes a set of rules and actions for excellence and trust in AI that guarantee the safety and fundamental rights of people and businesses, while strengthening investment and innovation across EU countries. The Commission's recent draft legislation takes these objectives a step further by proposing to turn Europe into "the global hub for trustworthy Artificial Intelligence (AI)" (European Commission 2021b). Biometric identification and specifically FRT have been central to many of the AI developments ranging from smart city initiatives financed by the EU all the way to the use of video surveillance and FRTs by law enforcement.

The implementation of the GDPR and the LED in the EU and EEA in May 2018 has set the scene for wide-ranging contestations over the use of surveillance technologies, specifically facial recognition technologies in public spaces. A number of influential reports have been published (FRA 2018; FRA 2019; CNIL 2019b; EDRi 2020; Fernandez et. al. 2020; González Fuster 2020), online campaigns launched (e.g., #ReclaimYourFace) to warn about the risks posed by AI while simultaneously trying to put pressure on the European Commission to address their impact on safety and fundamental rights. Although many of the issues put forward by these reports reflect the overarching concern with privacy issues and human rights violations, each organisation uses a different problem definition ranging from the technical challenges and limitations of AI all the way to the risks involved in the implementation of biometric technologies. As a consequence they also propose different mitigation strategies such as promotion with safeguards, moratorium or full ban. In what follows, we present the configuration of mobilisation and contestation.

FOUR POSITIONS IN THE POLICY DEBATES

Active promotion

A certain number of actors, both at the national and at the local level are pushing for the development and the extension of biometric remote identification. At the local level, the new technological developments meet a growing apetite for smart city initiatives and the ambitions of mayors that strive for developing digital platforms and employ technology-oriented solutions for governance and law enforcement. The intention of the mayor of Nice, Christian Etrosi, to make Nice a "laboratory" of crime prevention, despite repeated concerns of the French DPA, is a case in point (for a detailed analysis, see chapter 8 in this report, see also Barelli 2018). Law enforcement agencies across Europe also continue to press ahead with efforts to build digital and automated infrastructures that benefits tech companies who push their face recognition technologies with the concept of smart city and innovation tech (ex. Huawei, NEC, etc.).

At the national level, Biometric systems for the purposes of authentication are increasingly deployed for forensic applications among law-enforcement agencies in the European Union. As we elaborate in Chapter 3, 11 out of 27 member states of the European Union are

already using facial recognition against biometric databases for forensic purposes and 7 additional countries are expected to acquire such capabilities in the near future. The map of the European deployments of Biometric Identification Technologies (see Chapter 3) bear witness to a broad range of algorithmic processing of security images in a spectrum that goes from individual, localised authentication systems to generalised law enforcement uses of authentication, to Biometric Mass Surveillance.

Several states that have not yet adopted such technologies seem inclined to follow the trend, and push further. Former Belgian Minister of Interior Pieter De Crem for example, recently declared he was in favour of the use of facial recognition both for judicial inquiries but also for live facial recognition, a much rarer instance.

"The use of facial recognition can mean increased efficiency for security services […] The police are interested in using this technology in several of their missions. First of all, within the framework of the administrative police, with the aim of guaranteeing the security of a closed place accessible to the public, it would allow them to immediately intercept a person who is known in the police databases and who constitutes a danger for public security; but this technology can also be used within the framework of the judicial police, with the aim of controlling, during an investigation, if the suspect was present at the scene of the crime at the time when the punishable act was committed". (De Halleux 2020)
Such outspoken advocates of the use of RBI constitute an important voice, but do not find an echo in the EU mainstream discussions.

Support with safeguards
A second category of actors has indeed adopted the point of view that the RBI technologies should be supported, to the condition that their development should be monitored because of the risks they potentially pose. We find in this category the EU Commission, the EU Council, some EU Political parties, as well as the Fundamental Rights Agency (FRA), national DPAs such as the CNIL, the CoE (Council of Europe), and a certain number of courts.
Developments in the field of AI for governance, security and law enforcement are widely encouraged and financially supported by EU institutions. In their communication Shaping Europe's Digital Futures accompanying the White Paper on AI, the European Commission set out its guidelines and strategies to create a "Europe fit for the digital age" (European Commission 2020a). In support of a "fair and competitive economy" the Commission proposes a European Data Strategy (EDS) to make Europe a global leader in the data-agile economy. The EDS further aims to ensure Europe's technological sovereignty in a globalised world and "unlock the enormous potential of new technologies like AI" (Newsroom 2020). Therefore, the Commission proposes, among others "building and deploying cutting-edge joint digital capacities in the areas of AI, cyber, super and quantum computing, quantum communication and blockchain;" as well as "[r]einforcing EU governments interoperability strategy to ensure coordination and common standards for secure and borderless public sector data flows and services." (European Commission 2020a, 4)

The financial support for these initiatives is planned to be channelled from the Digital Europe programme (DEP), the Connecting Europe Facility 2 and Horizon Europe. Through the Horizon Europe for instance, the Commission plans to invest €15 billion in the 'Digital, Industry and Space' cluster, with AI as a key activity to be supported. The DEP would benefit from almost €2.5 billion in deploying data platforms and AI applications while also supporting na-

tional authorities in making their high value data sets interoperable (Newsroom 2020).
In the European Parliament, the EPPEuropean People's Party most aligns with this approach. “We want to regulate facial recognition technologies, not ban them. We need clear rules where they can be used and where they must not be used”, has for example declared Emil Radev MEP, EPP Group Member of the Legal Affairs Committee. As he puts it “Without a doubt, we want to prevent mass surveillance and abuse. But this cannot mean banning facial recognition all together. There are harmless and useful applications for facial recognition, which increase personal security" (European People’s Party, 2021)

The FRA’s 2019 report on facial recognition technologies (FRA 2019), which builds on several previous reports concerning biometrics, IT systems and fundamental rights (FRA 2018); big data and decision making (FRA 2018); data quality and artificial intelligence (FRA 2019); calls for a moderate approach. The FRA advocates for a comprehensive understanding of how exactly facial recognition technologies work and what their impact on fundamental human rights are. Fundamental rights implications of using FRT, they argue, vary considerably depending on the purpose, scope and context. They highlight a number of issues based on the EU fundamental rights framework as well as the EU data protection legislation. For example, according to Article 9 of the GDPR, processing of biometric data is allowed based on the data subject’s explicit consent, which requires a higher threshold of precision and definitiveness including for processing purposes. In terms of using biometric surveillance in public spaces, explicit consent would not provide a lawful ground for the relevant data processing because– as observed by the CJEU in its Schwarz decision, the data subject who is entering the premises would not have any choice of opting out of data processing. If the processing of biometric data is based on substantial public interest, which is another lawful data processing ground under Article 9 of the GDPR, it must be **“proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interest of the data subjects”** ((Article 9(2)(g), GDPR). Finally, when emphasising that the processing must be based on a lawful ground as recognised under the EU data protection legislation, the FRA was particularly vocal about the “function creep”, in regard to use of facial recognition systems and emphasised that the purpose of information collection must be strictly determined in light of the gravity of the intrusion upon people’s fundamental rights (25).

Therefore, the FRA places the right to privacy and protection of personal and sensitive data at the core of their problem definition, emphasising the potential dangers of FRTs undermining the freedom of expression, association and assembly. The FRA report also makes a case for the rights of special groups such as children, the elderly and people with disabilities, and addresses the issue of how the use of FRTs can contribute to further criminalise and stigmatise already discriminated groups of people (e.g., certain ethnic or racial minorities). In light of these considerations they advocate for a clear and “sufficiently detailed” legal framework, close monitoring and a thorough and continuous impact assessment of each deployment.

The French DPA, the CNIL, takes a similar position in the report “Facial Recognition. For a debate living up to the challenges” (CNIL 2019b). The CNIL report argues that the contactless and ubiquitous nature of the different FRTs can create an unprecedented potential for surveillance which, in the long run, could potentially undermine societal choices. They

also emphasise that biometric data is sensitive data therefore its collection is never completely harmless: "Even legitimate and well-defined use can, in the event of a cyber-attack or a simple error, have particularly serious consequences. In this context, the question of securing biometric data is crucial and must be an overriding priority in the design of any project of this kind" (CNIL 2019b, 6). In their recommendations, while calling for special vigilance, they acknowledge the legitimacy and proportionality of some uses. The CNIL pointed out that GDPR-endangering applications are often presented as "pilot projects", and thus requested the drawing of "some red lines even before any experimental use". They call instead for "a genuinely experimental approach" that test and perfect technical solutions that respect the legal framework (CNIL 2019b, 10).
The CoE's Practical Guide on the Use of Personal Data in the Police Sector (Council of Europe 2018), supplementing Convention 108+, puts great emphasis on implementing specific safeguards where an automated biometric system is introduced and considers that due to the high risk that such system poses to individuals' rights, data protection authorities should be consulted in its implementation (10). Also, as mentioned below, the Council of Europe's Guidelines on Facial Recognition (Council of Europe 2021), while considering a moratorium on the live facial recognition technology, sets out certain requirements to be met when implementing (possibly forensic) facial recognition technology.

Moratorium

On 20 January 2021, the European Parliament (2021) passed a resolution on artificial intelligence in which they invite the Commission "to assess the consequences of a moratorium on the use of facial recognition systems, and, depending on the results of this assessment, to consider a moratorium on the use of these systems in public spaces by public authorities and in premises meant for education and healthcare, as well as on the use of facial recognition systems by law enforcement authorities in semi-public spaces such as airports, until the technical standards can be considered fully fundamental rights-compliant, the results derived are non-biased and non-discriminatory, and there are strict safeguards against misuse that ensure the necessity and proportionality of using such technologies;" (European Parliament 2021).

Another authority calling for a moratorium on automated recognition technologies in public spaces is the European Data Protection Supervisor (EDPS), the independent supervisory authority with responsibility for monitoring the processing of personal data by the EU institutions and bodies. According to their 2020-2024 Strategy (EDPS 2020) "Shaping a Safer Digital Future" released on 30 June 2020, the EDPS stresses that they are committed to supporting the idea of a moratorium on "the deployment, in the EU, of automated recognition in public spaces of human features, not only of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, so that an informed and democratic debate can take place" (EDPS 2020).
The EDPS was also among the first to react to the draft Artificial Intelligence Act of the European Commission. While they welcomed the EU's leadership aiming to ensure that AI solutions are shaped according to the EU's values and legal principles, nonetheless they expressed their regret to see that their call for a moratorium on the use of remote biometric identification systems - including facial recognition - in publicly accessible spaces had not been addressed by the Commission. A stricter approach is necessary, they argue because "remote biometric identification, where AI may contribute to unprecedented developments, presents extremely high risks of deep and non-democratic intrusion into individuals' pri-

vate lives" (EDPS 2021). As mentioned below, shortly after their first reaction, the EDPS called for a general ban on the use of remote biometric systems with the European Data Protection Board (EDPB) (2021a).

A call for a moratorium, particularly, on facial recognition systems can be found in the Council of Europe documents. The Guidelines on Facial Recognition (Council of Europe, 2021) that is one of the instruments supplementing Convention 108+ call for a moratorium for the live facial recognition technologies (5) and lay out certain conditions for the use of facial recognition technologies by law enforcement authorities (6). For example, the Guidelines call for clear parameters and criteria when creating databases such as watchlists in light of a specific, legitimate, and explicit law enforcement purposes (ibid.)

Outright Ban

Finally, a certain number of EU Political Parties, EU and national NGOs have argued that there is no acceptable deployment of RBI, because the danger of Biometric Mass Surveillance is too high. Such actors include organisations such as EDRi, La Quadrature du Net, Algorithm Watch or the French Défenseur des Droits[1].

In the European Parliament, the European Greens have most vocally promoted the position of the ban, and have gathered support across party lines. In a letter to the European Commission dated 15 April 2021, 40 MEPs from the European Greens, the Party of the European Left, the Party of European Socialists, Renew Europe, a few non-attached MEPs and one member of the far-right party Identity and Democracy expressed their concerns about the leaked EU commission' proposal for the AI Regulation a few days earlier. As they argued

People who constantly feel watched and under surveillance cannot freely and courageously stand up for their rights and for a just society. Surveillance, distrust and fear risk gradually transforming our society into one of uncritical consumers who believe they have "nothing to hide" and - in a vain attempt to achieve total security - are prepared to give up their liberties. That is not a society worth living in! (Breyer et al. 2021)

Taking in particular issue with Article 4 and the possible exemptions to regulation of AI "in order to safeguard public safety", they urge the commissionEuropean Commission "to make sure that existing protections are upheld and a clear ban on biometric mass surveillance in public spaces is proposed. This is what a majority of citizens want" (Breyer et al. 2021)

European Digital Rights (EDRi), an umbrella organisation of 44 digital rights NGOs in Europe takes a radical stance on the issue. They argue that mass processing of biometric data in public spaces creates a serious risk of mass surveillance that infringes on fundamental rights, and therefore they call on the Commission to permanently stop all deployments that can lead to mass surveillance. In their report Ban Biometric Mass Surveillance (2020) they demand that the EDPB and national DPAs) "publicly disclose all existing and planned activities and deployments that fall within this remit." (EDRi 2020, 5). Furthermore, they call for ceasing all planned legislation which establishes biometric processing as well as the funding for all such projects, amounting to an "immediate and indefinite ban on biometric processing".

La Quadrature du Net (LQDN) one of EDRi's founding members (created in 2008 to "promote and defend fundamental freedoms in the digital world") similarly called for a ban on any present and future use of facial recognition for security and surveillance purposes. Together with a number of other French NGOs monitoring legislation impacting digital freedoms, as

1 The Defenseur des Droits is a governmental watchdog on civil rights and liberties in France. See Defenseur des Droits (2021) for the call for a ban on facial recognition.

well as other collectives, companies, associations and trade unions, the LQDN initiated a joint open letter in which they call on French authorities to ban any security and surveillance use of facial recognition due to their uniquely invasive and dehumanising nature. In their letter they point to the fact that in France there are a "multitude of systems already installed, outside of any real legal framework, without transparency or public discussion" referring, among others, to the PARAFE system and the use of FRTs by civil and military police. As they put it:

"Facial recognition is a uniquely invasive and dehumanising technology, which makes possible, sooner or later, constant surveillance of the public space. It creates a society in which we are all suspects. It turns our face into a tracking device, rather than a signifier of personality, eventually reducing it to a technical object. It enables invisible control. It establishes a permanent and inescapable identification regime. It eliminates anonymity. No argument can justify the deployment of such a technology." (La Quadrature du Net. et al. 2019)

Another prominent voice asking for a full ban on FRTs is the Berlin-based NGO Algorithm Watch. In their report Automating Society (2020) the NGO similarly calls for a ban to all facial recognition technology that might amount to mass surveillance. Their analysis and recommendations place FRTs in a broader discussion regarding Automated Decision-Making (ADM) systems. They condemn any use of live facial recognition in public spaces and demand that public uses of FRTs that might amount to mass surveillance be decisively "banned until further notice, and urgently, at the EU level" (Algorithm Watch 2020, 10).
They further demand meaningful transparency that not only means "disclosing information about a system's purpose, logic, and creator, as well as the ability to thoroughly analyse, and test a system's inputs and outputs. It also requires making training data and data results accessible to independent researchers, journalists, and civil society organisations for public interest research" (Algorithm Watch 2020, 11).

Parallel to these reports there are also various campaigns that prove to be effective in raising awareness and putting pressure on governmental bodies both at a national and European level. In May 2020 EDRi launched the #ReclaimYourFace campaign, a European Citizens' Initiative (ECI) petition, that calls for a ban on all biometric mass surveillance practices. The campaign centres around the power imbalances inherent to surveillance. As of May 2021 the campaign has been supported by more than 50.000 individual signatures. #ReclaimYourFace is not the only campaign, though undoubtedly the most visible and influential, in a European Contextcontext. Other similar international initiatives are: "Ban the Scan" initiated by Amnesty International, "Ban Automated Recognition of Gender and Sexual Orientation" led by the international NGO Access Now, or "Project Panopticon" launched by the Indian based Panoptic Tracker.

In early June; a global coalition was launched under the hashtag #BanBS consisting of 175 organisations from 55 countries the. The coalition demands the halting of biometric surveillance practices. Drafted by Access Now, Amnesty International, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF), and Instituto Brasileiro de Defesa do Consumidor (IDEC)), the open letter has been signed by almost 200 organisations, in which they call for an outright ban on uses of facial recognition and biometric technologies that enable mass surveillance and discriminatory targeted surveillance:
"These uses of facial and remote biometric recognition technologies, by design, threaten

people's rights and have already caused significant harm. No technical or legal safeguards could ever fully eliminate the threat they pose, and we therefore believe they should never be allowed in public or publicly accessible spaces, either by governments or the private sector." (Access Now 2021)

EU COMMISSION PROPOSAL ON THE REGULATION FOR THE ARTIFICIAL INTELLIGENCE ACT

The EU Commission Proposal

In April 2021, the European Commission (2021b) published its proposal on the Regulation for the Artificial Intelligence Act with the aim of setting out the harmonised regulatory rules for Member States on AI- based systems. It responded in part to the many challenges posed by the rapid technological development of AI as well as the pressure from watchdogs, regulatory bodies and civil society. If adopted in its current form, the proposed EU Artificial Intelligence Act will have important implications for the use of biometric identification systems for law enforcement purposes.

On the whole, the proposed EU Artificial Intelligence Act lays out those rules based on three categories of possible risks that the use of AI may create: (i) an unacceptable risk according to which the use of AI is prohibited (Article 5); (ii) a high-risk AI system, whose use is subject to certain conditions including an ex-ante conformity assessment (Article 6); and (iii) low or minimal risk, whose use is permitted without restrictions.

Notably for the purpose of this report, the proposed EU Artificial Intelligence Act covers "remote biometric identification systems" defined as "an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified" (Article 3(36)). In this way, the proposed EU Artificial Intelligence Act anticipates covering (AI-based) biometric video surveillance systems. In so doing, it differentiates between the use of "real-time" and "post" remote biometric identification systems in public spaces for law enforcement purposes.

On initial observation, the proposal prohibits the use of "real-time" (live) remote biometric identification systems in public spaces for law enforcement purposes because it classifies them as systems that create an unacceptable risk. However, Article 5 of the proposed EU Artificial Intelligence Act reads more as a heavy regulation rather than a prohibition. This is because the real-time remote biometric identification systems is prohibited unless it is "strictly necessary" for: (i) targeted search for specific potential victims of crime, including missing people; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; or (iii) in relation to a criminal offence for which a European Arrest Warrant can be issued provided that it is punishable by a custodial sentence or detention order of minimum three years. In determining the use of real-time remote biometric identification systems for one of those purposes, Member States should be subject to appropriate limits in time, space, and target person (Article 5(2)). A court or an independent administrative body should authorise the use of this type of biometric identification systems, except in duly justified emergency situations (Article 5(3)). Member States may allow for full or partial use of real-time biometric identification systems in public spaces for law enforcement purposes based on the requirements laid out in Article 5 of the Proposed Regulation (Article 5(4)).

The use of "post" (forensic) remote identification systems for law enforcement purposes,

on the other hand, is considered a high-risk AI system whose developers have the obligation to ensure that the system meets the condition set out in the proposed EU Artificial Intelligence Act (Chapter 2 and Annex III). As opposed to other high-risk AI systems whose providers have to conduct internal control checks, the post remote identification systems would be subject to third party conformity assessment.

The above provisions concerning the use of remote biometric identification systems have important implications on the protection of personal data and privacy as those systems involve processing of personal data. For this reason, they should be read alongside the rules and obligations set out in the GDPR and the LED. When conducted for law enforcement purposes by competent authorities, the remote biometric systems must follow the relevant data protection legislation as well as the ECHR and the Charter requirements since they would involve processing of sensitive personal data.

Reactions to the proposal

While data protection authorities and civil society generally welcomed the Commission's initiative praising its horizontal approach and the broad scope of its application, several organisations expressed their concerns that the regulations put forward are often far too lenient and do not do enough to safeguard fundamental rights. The EDPS (2021) for instance voiced its concern that the Commission did not address their call for a moratorium on the use of biometric identification, and specifically on facial recognition systems. Notably, in their later opinion on the proposed EU Artificial Intelligence Act with the EDPB (EDPS and EDPB 2021), they called for a general ban on the use of biometric identification (as opposed to their earlier calls on its moratorium). Both institutions were particularly vocal about the high regulation as opposed to the prohibition of the use of real-time remote biometric identification and they observed that the conditions for which the system could be implemented were extensive and would render the so-called prohibition meaningless (11).

They were also very critical of the distinction between real-time and ex-post (forensic) use of biometric identification systems, noting that the latter is as intrusive as the former because of its chilling effect on the freedom of expression, of assembly, of association and the freedom of movement (12). Furthermore, they highlighted the inherently intrusive nature of all types of remote biometric identification systems as they would involve indiscriminate and disproportionate amount of personal data of data subjects in public spaces to identify a few individuals (ibid). This would consequently impact people's reasonable expectation of anonymity in public spaces (ibid). For these reasons, the EDPS and the EDPB called for a general ban on 'any use of AI for an automated recognition of human features in publicly accessible spaces' (ibid).

The EDRi called the proposed EU Artificial Intelligence Act "a glimmer of hope for civil society who have called for red lines on impermissible uses of AI, like facial recognition in public spaces and predictive policing", however, defined the prohibitions proposed as "relatively feeble". They criticised in particular the many exemptions in which law enforcement agencies are still allowed to use "real-time remote biometric identification systems" (like facial recognition) in public spaces. These exceptions are targeted searches for specific potential victims of crime, to prevent a threat to life or terrorist attack, or to detect, localise, identify or prosecute a perpetrator or suspect of certain serious crimes (European Commission 2021b, 22). EDRi also points out that the Act "risks giving a green light to governments or public authorities to deploy discriminatory surveillance systems. Its rules for "high risk"

AI – like predictive policing, AI in asylum procedures and worker surveillance – fall mainly on the developers themselves, not the public institutions actually deploying them – a cause for concern." (EDRi 2021)

In June 2021 EDPB-EDPS also joined civil society in their call for a ban of automated facial recognition technologies (EDPB 2021a). In their joint opinion on the draft AI regulation (EDPB 2021a), they voice their concern of the exclusion of international law enforcement cooperation from the scope of the AI Proposal. While the EDPB and the EDPS welcome the risk-based approach underpinning the Proposal, they consider the concept of "risk to fundamental rights" as one which should be aligned with the EU data protection framework and the societal risks for groups of individuals should also be assessed and mitigated. Therefore, they call for "a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context." (EDPB 2021a))

PART 2
CASE STUDIES

CHAPTER 6

FACIAL RECOGNITION CAMERAS AT BRUSSELS INTERNATIONAL AIRPORT (BELGIUM)

FACIAL RECOGNITION CAMERAS AT BRUSSELS INTERNATIONAL AIRPORT (BELGIUM)

Key points

- Belgium is one of two European countries that has not yet authorised the use of FRT, however, law enforcement is strongly advocating for its use and the current legal obstacles to its implementation might not hold for very long given the political pressure.
- In 2017, unbeknownst to the Belgian Supervisory Body for Police Information (COC), Brussels International Airport acquired 4 cameras connected to a facial recognition software for use by the airport police. Though the COC subsequently ruled that this use fell outside of the conditions for a lawful deployment, the legality of the airport experiment fell into a legal grey area because of the ways in which the technology was deployed.
- One justification for the legality of the airport experiment from the General Commissioner of Federal Police was to compare the technological deployment to that of the legal use of other intelligent technologies such as Automated Number Plate Recognition (ANPR). Although this argument was rejected at the time, such a system could be re-instated if the grounds for interruption are no longer present in the law.
- Some civil society actors in Belgium contest the legitimacy of remote biometric identification. However, current legislative activity seems to point in the direction of more acceptance for remote biometric surveillance.

Belgium is, with Spain, one of the few countries in Europe that has not authorised the use of facial recognition technology, neither for criminal investigations nor for mass surveillance . This does not mean that it is unlikely to change its position in the very near future. Law enforcement is indeed strongly advocating its use, and the current legal obstacles are not likely to hold for very long . The pilot experiment that took place in Zaventem / Brussels International Airport, although aborted, occurred within a national context in which biometric systems are increasingly used and deployed.

Belgium will, for example, soon roll out at the national level the new biometric identity card "eID", the Minister of Interior Annelies Verlinden has recently announced. The identification document, which will rely on the constitution of a broad biometric database and is part of a broader European Union initiative, is developed in partnership with security multinational Thales, was already trialled with 53.000 citizens in (Prins 2021; Thales Group 2020)[1].

Municipalities in different parts of the country are experimenting with Automated Number Plate Recognition (ANPR) technology. A smaller number have started deploying "smart CCTV" cameras, which fall just short of using facial recognition technology. The city of Kortrijk has for example deployed "body recognition" technology which uses walking style or clothing of individuals to track them across the city's CCTV network[2]. Facial recognition is possible with these systems, but has not been activated as of yet pending legal authorisation to do so. In the city of Roeselare, "smart cameras" have been installed in one of the shopping streets. Deployed by telecom operator Citymesh, they could provide facial recognition services, but are currently used to count and estimate crowds, data which is shared with the police . All the emerging initiatives of remote biometric identification are however pending a reversal of the decision to halt the experiment at Zaventem Brussels International Airport.

THE ZAVENTEM PILOT IN THE CONTEXT OF FACE RECOGNITION TECHNOLOGY IN BELGIUM

The use of facial recognition technology at the Brussels International Airport was announced on 10 July 2019 in the Flemish weekly Knack by General Commissioner of Federal Police Marc De Mesmaeker There is currently no publicly available information as to whom provided the technical system. De Mesmaeker explained that an agreement had been found with the company managing the airport and the labour unions, and thus that the technology was already in use .

As part of the justification for the deployment of FRT in Zaventem, De Mesmaeker made a comparison with ANPR-enabled cameras, arguing that "They have already helped to solve investigations quickly, (…). Citizens understand this and have learned to live with their presence, but privacy remains a right".
The Belgian Supervisory Body for Police Information (COC)[3], in its advisory document, explained that it had no prior knowledge of the deployment and learned about the existence of the facial recognition systems through the interview of De Mesmaeker in the Knack magazine . On 10 July 2019, the COC thus invited the General Commissioner to communicate all the details of the deployment of this techno-

1 While the eID project is not specific to Belgium, the country stands out for having piloted the project ahead of other EU member states. eID is a form of authentication rather than surveillance system - yet the constitution of a database of machine-readable identities participates to the construction of a digital infrastructure of surveillance that can be misuedmisused for biometric mass surveillance., as argued in chapter 3

2 The technology is provided by RTS, a security technology reseller.

3 The COC, or Supervisory Body for Police Information is « the autonomous federal parliamentary body in charge of monitoring the management of police information and also the data controller for the integrated police service, the Passenger Information Unit and the General Inspectorate of the Federal and the Local Police. » (Organe de Controle de l'Information Policière 2021).

logy in the Brussels International Airport. On 18 July 2019, COC received a summary of the system's main components. On 9 August 2019, it subsequently visited the premises of the federal police deployment in Zaventem airport .
We know some technical details about the system through the public information shared by the COC. In early 2017, Brussels airport had acquired 4 cameras connected to a facial recognition software for use by the airport police (Police Aéronautique, LPA) . The system works in two steps.

When provided with video feeds from the four cameras, the software first creates snapshots, generating individual records with the faces that appear in the frame. These snapshots on record are then in a second step compared and potentially matched to previously established "blacklists" created by the police itself (the reference dataset is thus not external to this particular deployment) .

The system did however not live up to its promise and generated a high number of false positives. Many features such as skin colour, glasses, moustaches, and beards led to false matches. The system was thus partially disconnected in March 2017, and at the time of the visit of the COC, the system was no longer fully in use . Yet the second step had not been de-activated (matching video feeds against pre-established blacklists of faces), the first function of creating a biometric record of the video feeds was still in place .

LEGAL BASES AND CHALLENGES

The legality of the Zaventem airport experiment fell into a legal grey area, but eventually the COC ruled that it fell outside of the conditions for a lawful deployment.
The right to privacy is enshrined in Article 22 of the Belgian Constitution, which reads as "everyone has the right to the respect of his private and family life, except in the cases and conditions determined by the law." The ECHR and the case law of the ECtHR have had considerable influence over the interpretation of Article 22 of the Belgian Constitution (Lavrysen et al. 2017) and thus the right enshrined therein can be broadly construed to encompass the right to protection of personal data and to address risks associated with the use of new technologies (Kindt et al. 2008; De Hert 2017). Articles 7 and 8 of the Charter are also relevant where the legislator acts within the scope of EU law (Cour constitutionnelle, N° 2/2021, 14 January 2021).

Belgium adapted its data protection law to the GDPR by enacting the Act of 30 July 2018 on the Protection of Natural Persons with regard to the Processing of Personal data (the Data Protection Act). The same act implements the LED, as well.

In regard to processing of sensitive data for non-law enforcement purposes, the Act sets out certain processing activities which would be regarded as necessary for reasons of substantial public interest, which is one of the lawful grounds listed in Article 9 of the GDPR to process said data. Overall, the relevant public interest purposes relate to processing by human rights organisations in relation to their objective of defending and promoting human rights and fundamental freedoms and in relation to an offence in relation to missing persons or sexual exploitation (Article 8, §1, the Data Protection Act). A separate data processing purpose for personal data of sexual life of the data subject is introduced in relation to the statutory purpose of evaluating, supervising, and treating persons whose sexual behaviour may be qualified as a criminal offence (Article 8, §1, 3°, the Data Protection Act).

Biometric data, however, cannot be processed by the respective associations for said public interest purpose unless specified in legal pro-

visions (Article 8, §1, the Data Protection Act). More importantly when biometric data is processed (not limited to the reasons of public interest), there must be additional safeguards whereby the data controller designates the categories of people who have access to the data, keeps a record of people who have access to the data for the data protection authority, and makes sure that they are bound by a legal, statutory or contractual obligation of confidentiality with respect to the personal data that they process (Article 9, the Data Protection Act).

The Act further provides a number of lawful bases for which sensitive data may be processed for law enforcement purposes as specified in Article 10 of the GDPR. The legal bases include processing as authorised by law, decree, ordinance, EU law or international agreement, necessary for protecting the vital interests of the data subject or another, in relation to data that is made public (Article 34, the Data Protection Act). Competent authorities have the same obligations of compiling a list of persons who have access to the data and are bound by obligations of confidentiality (Article 34, §2, the Data Protection Act).

Pursuant to Article 23 of the GDPR, the Act provides exceptions to the data subject's rights when personal data are processed by a range of authorities specified therein including the police services (Title I, Chapter III, the Data Protection Act) and intelligence and security services (Title III, the Data Protection Act). Particularly in the context of data processing for law enforcement purposes, pursuant to Article 35 of the Act, the sole automated decision making is permitted if the law, the decree, the ordinance, the EU legislation, or the international agreement provides for appropriate safeguards for the rights and freedoms of the data subject, including at least the right to human intervention on the part of the controller. However, profiling that leads to discrimination based on the sensitive data is prohibited (Article 35, the Data Protection Act).

In March 2018, Belgium amended its law on the use of surveillance cameras, particularly the Police Act (Loi sur la fonction de police/ Wet op het politieambt) to regulate the use of cameras by the police. Accordingly, it provided new rules on the use of mobile cameras (caméra mobile/mobiele camera) and smart cameras (caméra intelligente/intelligente camera) equipped with additional technology that is beyond simple processing of images such as facial recognition cameras or automatic number plate recognition, as acknowledged in the Parliamentary Document No. 54 2855/001 of 4 January. The amendment to the Act permits the use of real-time smart cameras by the police in carrying out their administrative and judicial duties (subject to when they are to be used in public, in enclosed places freely accessible by the public or not).

According to the amended Act, the personal data collected by cameras can be retained for a maximum period of 12 months (Article 25/5, Police Act). During this period, access to the data is allowed for a period of one month from their registration and subject to a written and reasoned decision of the public prosecutor (Procureur du roi/Procureur des Konings) (Article 25/6, Police Act). When cameras are used visibly in administrative as well as judicial missions of the police (e.g., maintaining public order, crowd management etc.) (ibid), they should not be aimed at collecting information about a person's racial or ethnic origin, religious or philosophical beliefs, political views, trade union membership, health status, sex life or sexual orientation (Article 25/3, §3, Police Act). Interestingly, biometric data is not included in this list of information whose collection by means of cameras are prohibited. The Police Act further sets out the police powers to col-

lect information about people and it provides that biometric data that categorises different data subjects such as those who committed an offence against maintaining public order or for whom there is a monitoring order can be processed solely for the identification of those subjects (Article 44/1, the Police Act). If such processing is likely to generate a high risk to the rights and freedoms of the persons concerned, the police must consult the Belgian Supervisory Body for Police Information (ibid).

MOBILISATIONS AND CONTESTATIONS

Based on this legislative framework, the General Commissioner, in his letter to the COC dated 18 July 2019, justified a deployment without consultation of the COC nor the Belgian DPA on the grounds that:

"although the creation of a technical database for facial recognition is not possible under the current legislation, the use of real-time intelligent technologies other than Automatic Number Plate Recognition (ANPR) is possible under Article 25/3 of the LFP. The legislator has indeed provided that a camera used by the police, regardless of its type, can be equipped with intelligent technology. The introduction of real-time facial recognition is therefore, in our opinion, in accordance with the law."

The COC was not convinced by the arguments of the General Commissioner and concluded that the LFP did not apply. It justified its decision as follows:

"As the case stands, the Regulator is not entirely convinced that the LFP is applicable. It is true that the definition of a "smart camera" is taken in a very broad sense. According to Article 25/2, §1, 3° of the LFP, this term refers to "a camera which also includes components and software which, whether or not coupled with registers or files, can process the images collected autonomously or not". In the explanatory memorandum, ANPR cameras and cameras for facial recognition are mentioned as examples It further added that:

The possibility of testing a facial recognition system first raises questions about the exact scope of the processing. When determining the correct legal framework, it is not possible to establish from the outset whether the processing of personal data in the context of research and prosecution is already being considered in the test environment or during a test period - and thus whether the FPA and Title II of the DPA apply. The answer to this question is crucial in order to determine the legal basis, the level of decision making within the police that is entitled to decide to use facial recognition, the nature of the storage medium and the duration of storage, and the level of information security to be observed (operational or not). Secondly, and in the alternative, the Review Body notes that the LFP, if applicable, does describe what falls under the definition of a smart camera, but does not stipulate in what circumstances and under what conditions the use of facial recognition cameras is permitted, let alone on what medium the images can/should be recorded and what data should at least be stored. In the current state of the legislation, the legislator only wanted to regulate the creation of a technical database for ANPR images. (Organe de Controle de l'Information Policière 2019, 4)

The COC thus counter-argued that because the current CCTV law was not voted on with facial recognition but ANPR in mind, and facial recognition is permitted but only for commercial use (such as the check-in of passengers) it was thus not legal to set up a technical database containing biometric information and the system did therefore not have a sound legal basis . The interesting technicality of the case is that the "snapshots" generated in the first phase of the system's workflow were in practice stored only for a fraction of a second. Yet according to the law, this is still a biometric

database, and thus not allowed .

The reaction by the Belgian Supervisory Body for Police Information shows that a degree of unclarity on the legal basis for conducting biometric surveillance persists. From a legislative perspective, such a system can easily be re-activated if the grounds for the interruption are not present in the law anymore. The current legislative activity seems to point in this direction.

EFFECTS OF THE TECHNOLOGIES

While the city of Brussels is the location of much EU-level activism, this hasn't translated yet in an equal mobilisation at the national level – perhaps due to the currently very restrictive legislative position on the matter and the institutional checks and balances described in this chapter – banning de facto the use of such technologies.

The French campaign Technopolice has extended to Belgium and is raising awareness through a diversified strategy based on public forums, cartography of technology and organization of events. The NGO Ligue des Droits Humains is a member of the Reclaim Your Face campaign, along with 40 other organisations[4], yet it hasn't been as active as partner organizations in neighbouring France or Germany.

4 https://reclaimyourface.eu/

CHAPTER 7

THE BURGLARY FREE NEIGHBOURHOOD IN ROTTERDAM
(NETHERLANDS)

THE BURGLARY FREE NEIGHBOURHOOD IN ROTTERDAM (NETHERLANDS)

Key points

- The Fieldlab Burglary Free Neighbourhood is a public-private collaboration with two aims: to detect suspicious behaviour and to influence the behaviour of the suspect. While the system of smart streetlamps does collect some image and sound-based data, it does not record any characteristics specific to the individual.
- From a legal perspective, there is a question as to whether or not the data processed by the Burglary Free Neighbourhood programme qualifies as personal data and thus would fall within the scope of data protection legislation.
- It is contested whether forms of digital monitoring and signalling are actually the most efficient methods for preventing break ins. Despite the aims of the programme, to date, the streetlights have only been used to capture data for the purposes of machine learning.
- The infrastructure installed for the experiments can potentially be used for more invasive forms of monitoring. During the project, local police, for example, already voiced an interest in access to the cameras.
- In March 2021, the Fieldlab trial ended. The data collected over the course of the project was not sufficient enough to have the computer distinguish suspicious trajectories. The infrastructure of cameras and microphones is currently disabled, yet remains in place.

In October 2019, the Carlo Collodihof, a courtyard in the Rotterdam neighbourhood Lombardijen, was equipped with a new kind of streetlamp. The twelve new luminaires did not just illuminate the streets; they were fitted with cameras, microphones, speakers, and a computer which was connected to the internet. They are part of the so called Fieldlab Burglary Free Neighbourhood: an experiment in the public space with technologies for computer sensing and data processing, aimed at the prevention of break-ins, robberies, and aggression; increasing the chances of catching and increasing a sense of safety for the inhabitants of the neighbourhood ((Redactie Inbraakvrije Wijk 2019; Kokkeler et al. 2020b). The practical nature of a Fieldlab provides a way to examine concretely how the various technologies come together, and how they fit in with existing infrastructures and regulations.

DETECTION AND DECISION-MAKING IN THE "BURGLARY FREE NEIGHBOURHOOD" FIELDLAB

The national programme Burglary Free Neighbourhood was initiated and funded by the Dutch Ministry of Justice and Security. It is led by DITSS (Dutch Institute for Technology, Safety & Security), a non-profit organisation, that has been involved in earlier computer sensing projects in the Netherlands – for example in Stratumseind, Eindhoven (The Hague Security Delta 2021). Other parties involved include the municipality of Rotterdam, the police –both on a local and national level– the Public Prosecutor's Office and insurance company Interpolis. Part of the research is carried out by University of Twente, Avans Hogeschool, the Network Institute of the Vrije Universiteit Amsterdam and the Max Planck Institute for Foreign and International Criminal Law (Freiburg, Germany).

From a technological perspective, the project has two aims: to detect suspicious behaviour, and in turn, to influence the behaviour of the suspect. As such, project manager Guido Delver, who agreed to be interviewed for this report, describes the project as being primarily a behavioural experiment (Delver 2021). The twelve luminaires are provided by Sustainder (their Anne series (Sustainder 2021)). The processing of the video and audio is done on the spot by a computer embedded in the

Figure 2. *Fieldlab in Rotterdam Lombardijen*

luminaire, using software from the Eindhoven based company ViNotion (ViNotion 2020). This software reads the video frames from the camera and estimates the presence and position of people – thereby mapping the coordinates of the video frame to coordinates in the space. It then determines the direction they are facing. Only these values –position and direction– and no other characteristics nor any images, are sent over the internet to a datacentre somewhere in the Netherlands, where the position data is stored for further processing (Delver 2021).

Currently, there is no immediate processing of the position data to classify behaviour as being suspicious or not. The proposed pipeline consists of two stages: first, an unsupervised machine algorithm for anomaly (outlier) detection processes the gathered trajectories, in order to distinguish trajectories that statistically deviate from the norm. As an example, both children playing, as well as burglars making a scouting round through the neighbourhood can potentially produce anomalous trajectories. Secondly, these anomalous trajectories are judged as being suspicious or not by a computer model that was trained with human supervision. In the Fieldlab's first data collection experiment 100.000 trajectories were collected, totalling 20.000.000 data points (Hamada 2020). It turned out however that this was still too few to draw any conclusions about viability of the approach; the big data was still too small (Delver 2021).

Another input for detecting suspicious situations is the microphone with which some of the streetlamps are equipped. By recording two frequencies of sound, sounds can be categorised as coming from for example a conversation, shouting, dog barking, or the breaking of glass. The two frequencies recorded provide too little information to distinguish the words in a conversation (Delver 2021).
Aside from experimenting with the automated detection of suspicious behaviour, the Fieldlab experiments with various ways in which the detected situations can be played out. Project manager Guido Delver notes that the aim is not per se to involve the police. Instead, the suspect should be deterred before any crime is committed (Delver 2021). Various strategies are laid out: the yet-to-be-autonomous system can voice warnings through the speakers embedded in the streetlamps. Or, in line with the work of DITSS in Eindhoven's Stratumseind street, the light intensity or colour of the streetlamps can be changed (Intelligent Lighting Institute, n.d.). Both strategies are aimed at signalling the subjects that their behaviour is noticed, which generally suffices to have burglars break off their scouting. Another option under consideration is to send a signal to the residents living nearby.

The process of data gathering in the Burglary Free Neighbourhood is quite similar to technologies that are deployed for anonymous people counting. One such application has been developed by Numina and is deployed in the Dutch city of Nijmegen: individuals are traced through space and time, but not identified or categorised. This information is then used to provide statistics about the number of visitors in the city centre (Schouten and Bril 2019). Another Dutch deployment of technologically similar software is the One-and-a-half-meter monitor developed by the municipality of Amsterdam, which is based on the YOLO5 object detection algorithm and trained on the COCO dataset. This data processing architecture can detect the presence of persons but is incapable of deducing any characteristics (Amsterdam-Amstelland safety region 2020). These implementations show biometrics can be used to detect the presence of people, while refraining from storing these characteristics.

LEGAL BASES AND CHALLENGES

The Fieldlab Burglary Free Neighbourhood programme shows how data can be used to conduct monitoring and nudging of individuals' behaviours. From a legal point of view, the question is whether the data processed in the context of the programme qualifies as personal data and would thus fall within the scope of data protection legislation.

The Constitution for the Kingdom of the Netherlands provides for a general right to protection for privacy in Article 10, according to which restrictions to that right must be laid down by law. The GDPR Implementation Act (Uitvoeringswet Algemene Verordening Gegevens-bescherming) (UAVG), as well as the Police Data Act (Wet Politiegegevens) or the Judicial Data and Criminal Records Act (Wet Justitiele en Strafvorderlijke Gegevens) which implement the GDPR and the LED, provides the legal framework regarding privacy and data protection.

The definition of personal data as enshrined in the GDPR and the LED is directly applicable under the Dutch law. To qualify data as such, "any information" must relate to an identified or identifiable natural person. Based on the data that can be captured by the Fieldlab programme, two elements of this definition need further attention.

-"Information "relating to" a natural person". The former Article 29 Working Party (2007) substantiated this element by noting that information can relate to an individual based on its content (i.e., information is about the individual), its purpose (i.e., information is used or likely to be used to evaluate, treat in a way, or influence the status or behaviour of an individual), or its result (i.e., information is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case). These three alternative notions to determine whether the information relates to an individual was endorsed by the CJEU in its Nowak decision (C-434/16), where it dealt with the purpose (i.e., it evaluates the candidate's competence) and the result (i.e., it is used to determine whether the candidate passes or fails, which can have an impact on the candidate's rights) of the information in question in determining whether the written answers to an exam would qualify as personal data. In brief, in determining whether the data captured by the Fieldlab programme qualify as personal data, the context for which the data is used or captured is important. Information about the level of crowding or sound could "relate" to an individual if it is used to evaluate or influence the behaviour of a person (based on its purpose), or to affect a person's rights (based on its result) (Galič and Gellert 2021).

-"Identifiable Person". The notion of identifiability covers circumstances where it is possible to distinguish the individual from a group of people by combining additional information (See 4.2.1). In situations where the person cannot be identified, determining the extent to which that person can be identifiable depends on the possibilities of combining additional identifying information (Galič and Gellert 2021). However, where the system mainly operates on non-personal data because its aim is to influence the behaviour of a group of people, instead of an identified or identifiable person, the chances of having sufficient data to render the person identifiable would be lower (ibid).

The uncertainties around these two elements of personal data mean that a project that monitors and tracks the behaviour of individuals in public spaces may fall outside the scope of data protection legislation if there are uncertainties around whether the data it processes actually qualify as personal data. Notably, the

Whitepaper on the sensors in the role of municipalities (van Barneveld, Crover, and Yeh 2018), produced in collaboration with the Ministry of Interior, a reference to the definition of personal data and the possibility of combining for example sound-data with camera recordings to trigger the application of the data protection legislation, without giving further details. Unlike in the relevant sections of the other case studies, this section will not explore further data processing conditions under the UAVG and the other relevant laws because the issue from a data protection view in the first instance with the Fieldlab programme or any similar initiative is whether they process personal data.

MOBILISATIONS AND CONTESTATIONS

Despite visits from the mayor of Rotterdam and Secretary of State Sander Dekker, the Fieldlab of the Burglary Free Neighbourhood has not been discussed much in Dutch media. The most prominent discussion on the project has been in a TV broadcast and online video by Nieuwsuur, in which criminologist Marc Schuilenburg is sceptical about the technology deployed in the Fieldlab (Nieuwsuur 2020a, 5:38m):

So far, there has not been any study that assesses the effectiveness of the streetlamps. We know what works best against burglary: looking out for each other and fitting your door with a double lock. Social cohesion is known to work best. […] What is happening now is that social cohesion is degrading, because neighbours can trust in the intelligent streetlight. Any responsibility is delegated to a streetlight.

Schuilenburg frames the interest of cities in technologies such as those used in the Burglary Free Neighbourhood as being part of the well-marketed narrative of the "smart city" that is sold by technology companies: "no city wants to be dumb" ("Nieuwsuur" 2020b, 36m). To some extent, Guido Delver positions the project's privacy-by-design methodology in contrast to many of these commercial products for surveillance. In his conversations with various municipalities he recognises, and shares, the interest for "smart" surveillance technologies. However, Delver attempts to minimise the data gathering in the Burglary Free Neighbourhood. This proves to be a constant negotiation, for example the police have voiced an interest in access to the camera feeds in case suspicious behaviour was detected. However, access to the camera feeds has been deliberately kept outside of the scope of the project (Delver 2021).

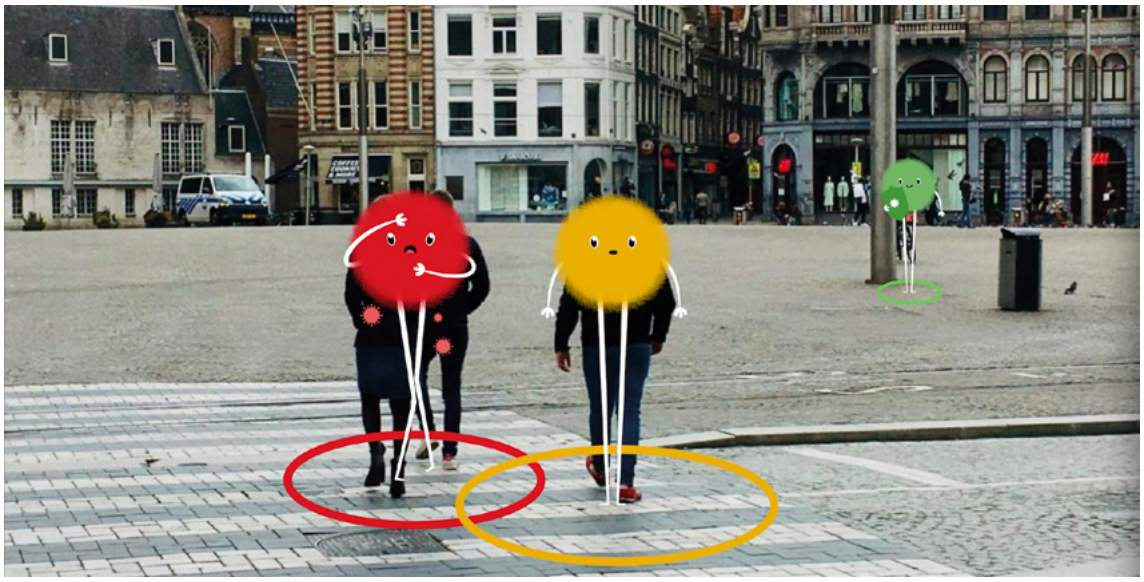


Figure 3. *The one-and-a-half-meter monitor developed by the municipality of Amsterdam*

While the project currently only stores the position of passers-by, there are also technical considerations for the capture of more information. For example, the video cameras cannot cover the entire area, therefore, as no characteristics of individuals are stored, tracking people from one camera to the next is problematic. It raises the question of whether biometric measurements such as a person's estimated volume, length, or colour of clothing should be recorded, this would allow the computer to link the trace of one camera to another. Posing ethical and legal questions for the project: what are the legal ramifications of deducing and (temporarily) storing these characteristics, and for how long should they be stored (Delver 2021)? Even for projects that decide to consider privacy by design, it can be tempting to store and process biometric information. However, as mentioned above (see section 7.2.), the challenges in determining whether the Fieldlab or any other similar initiatives process personal data as defined in the GDPR raises questions on the extent to which these programmes fall within the scope of the data protection legislation, irrespective of the fact that they may be designed to affect the personal autonomy of individuals (as opposed to an identified or identifiable individual) by influencing and nudging their behaviours.

Finally, commentators have pointed out the discrepancy between what is expected of the technology, and what it is actually doing. For example, the Algemeen Dagblad (Krol 2019) writes that the "smart streetlights" are actually able to "recognise behaviour" and to "sound the alarm" if necessary. Whereas up until now, the streetlights have only been used to capture data for machine learning.

These observations raise the question as to whether or not the communication about the technologies used suffices. When entering the neighbourhood, a sign signals to the visitor that the Fieldlab is operative, however, much of the information discussed above could not be found on the website that is mentioned on the sign – as is indicated by the breath of references used. This situation is substantially different from the way that, for example, the city of Amsterdam lays out its use of algorithms: one website presents the goals of the projects, the kinds of data processing that is happening, the datasets on which the algorithms are trained, and in some cases the source code is shared (Amsterdam Algoritmeregister, 2021). The Dutch government is currently drafting regulations for a national register of cameras and sensors as deployed by municipalities (Nieuwsuur 2020b).

EFFECTS OF THE TECHNOLOGIES

Since March 2021, the experiment in the Fieldlab of the Burglary Free Neighbourhood in Rotterdam has been on hold. Researchers have not yet been able to have the computer distinguish suspicious trajectories or sounds. As such, the system has not been able to respond to any such situations with lights or sounds (Redactie LikeJeWijk 2021). Further research into this is happening in a Virtual Reality environment, as was discussed in the first section.

As part of the Fieldlab, research about the effects of the technologies deployed in the streets has been carried out by the Avans Hogeschool, presenting five relevant observations. First, it is too early to draw any conclusions about the impact of the deployed technologies on the statistics for high impact crime (e.g., break-ins, aggression, robberies) in the neighbourhood (Kokkeler et al. 2020b, 25). Moreover, no research has yet been done into the waterbed effect of crime – whether crime prevention in one block, leads to an increase in crime in an adjacent neighbourhood (Kokkeler et al. 2020b, 9).

Secondly, in the Rotterdam neighbourhood that was examined, the streetlights equipped with cameras were by no means the only technological interventions to prevent break-ins. A breadth of technology is deployed –e.g., cameras, alarm systems– which are either privately owned, owned by the municipality, the police, or distributed by insurance companies. In this cacophony of technological appliances, it becomes unclear which data is collected and how it is processed. Furthermore, it is unclear who owns and manages these data collection and processing networks, whether they are private parties or law enforcement agencies. Kokkeler et al. argue that a better overview of these practices is crucial in order to assess the ethical, legal, and social impact of these deployments (Kokkeler et al. 2020b, 24).

Thirdly, after conducting interviews with the residents, Kokkeler et al. concluded that most were unaware that the newly placed streetlights were equipped with sensors. Moreover, when discussing the "sensors" in the streetlights, many residents could only imagine the use of cameras – not realising what data was being gathered (Kokkeler et al. 2020a, 21). While resident participation features prominent in the goals of the Fieldlab, the Coronavirus pandemic has hindered the planned involvement of the residents (Delver 2021).

Fourth, the moment residents were informed about the data gathering and processing taking place, they were optimistic about a potential use of the data by the local police and municipality. As long as the cameras were only directed at public space. Some residents voiced their concern that the information should only be used to address high impact crime, and not for minor offences – in particular if these involve minors. On the other hand, some other residents suggested a broader use of the streetlights, for example in fighting litter and speeding (Kokkeler et al. 2020a, 21). Despite the fact that the direct sharing of the generated data with the police is contrary to the aims of the project (Delver 2021) the infrastructure that is deployed in the streets enables other engagements with the technology – the so-called function creep.

Finally, the residents of the Rotterdam neighbourhood are known to not properly use more "low-tech" security measures. A case in which someone went out to walk their dog while leaving the key in the door is an illustration of this. Moreover, when a break in happens, it is not always reported, as often the culprit is directly or indirectly known (Kokkeler et al. 2020a, 22). This indicates that the technologies used in the Fieldlab might be unfit to address the primary issues in the neighbourhood.

All in all, the case of the Fieldlab Burglary Free Neighbourhood provides for interesting and relevant research into alternative means of behavioural monitoring and influencing. The direct "nudging" of behaviour theoretically removes the need for a centralised database of biometric data, it also does not capture and process biometric information on individuals. Yet in order to increase detection capabilities, it can be a slippery slope to implement algorithmic deduction of individuals' traits, while storing these for short amounts of time. However, for how long should this information be kept? In other words: what is the desired balance between increased detection performance and storage duration. In this light, the project's current setup of not storing, nor deducing any biometric information is a clear, fixed, guideline that avoids this grey zone and many of the issues with remote biometric identification that are addressed within this report.

It is however apparent that projects such as these require (legal) fail-safes for their usage. In the case of the Burglary Free Neighbourhood, it seems the project's privacy-by-design has been secured by project manager Delvers. The fact that local police requested access to the cameras indicates the necessity for proper

oversight in such deployments. Assuming that the data protection legislation applies to the Fieldlab or any similar initiatives (to the extent that they process "personal data"), it is unclear as to who processes which type of data and the level of collaboration between the private and public sectors. This uncertainty means that it may be hard to allocate responsibilities and obligations under the data protection legislation since it may be complicated to determine who is the "competent authority", whose processing activities in a law enforcement context fall under the scope of the LED, as well as who is the authority responsible for processing personal data (i.e., the data controller) and the one responsible for processing the data on behalf of that authority (i.e., the data processor). Such uncertainties may complicate the effectiveness of the data protection legislation (Purtova, 2018).

CHAPTER 8

THE SAFE CITY PROJECTS IN NICE (FRANCE)

THE SAFE CITY PROJECTS IN NICE (FRANCE)

Key points

- Several French cities have launched "safe city" projects involving biometric technologies, however Nice is arguably the national leader. The city currently has the highest CCTV coverage of any city in France and has more than double the police agents per capita of the neighbouring city of Marseille.
- Through a series of public-private partnerships the city began a number of initiatives using RBI technologies (including emotion and facial recognition). These technologies were deployed for both authentication and surveillance purposes with some falling into the category of biometric mass surveillance.
- One project which used FRT at a high school in Nice and one in Marseille was eventually declared unlawful. The court determined that the required consent could not be obtained due to the power imbalance between the targeted public (students) and the public authority (public educational establishment). This case highlights important issues about the deployment of biometric technologies in public spaces.
- The use of biometric mass surveillance by the mayor of Nice Christian Estrosi has put him on a collision course with the French Data Protection Authority (CNIL) as well as human rights/ digital rights organisations (Ligue des Droits de l'Homme, La Quadrature du Net). His activities have raised both concern and criticism over the usage of the technologies and their potential impact on the privacy of personal data.

Although several French cities such as Paris, Valenciennes or Marseille have launched pilot projects for "safe city" projects involving biometric technologies (facial, voice, sound recognition), the city of Nice is perhaps the national leader in the experimentation with such technologies at a local level (Nice Premium 2017). The mayor of Nice, Christian Estrosi (Les Républicains Party, right) a prominent political figure on the national political scene, has made clear his intention was to make Nice a "laboratory" of crime prevention (Barelli 2018). Since 2010, more than 1.962 surveillance cameras have been deployed throughout the city, making it the city with highest CCTV coverage in France (27 cameras per square meter). Nice also possesses the most local police in France per inhabitant: 414 agents, for a population of 340.000 (in comparison, the neighbouring city of Marseille has 450 agents for 861.000 inhabitants).

THE VARIOUS FACETS OF THE "SAFE CITY" PROJECT IN NICE

Nice has experimented with various initiatives related to remote biometric identification – many of which fall into the category of biometric mass surveillance. In 2017, Christian Estrosi announced a partnership with the energy company Engie Ineo for the development of an Urban Surveillance Centre (Centre de Surveillance Urbain, CSU). Based on a touch-interface technology, it centralises a platform of real-time data such as traffic accidents, patrol locations, as well as video feeds from CCTVs on the streets and in public transportation. (Dudebout 2020, 1). The video feeds from the city tramways are connected to an emotion recognition algorithm to flag suspicious situations (Allix 2018).

In June 2018, an additional step was taken with the signing of a partnership agreement with a consortium of companies headed by Thales, specialised in social network intelligence, geolocation, biometrics and crowd simulation[1] for a "Safe City" project (Dudebout 2020, 2). Established for three years (2018-2021) with a budget of EUR 10,9 million, the project is financed by the city council, subsidised in part by BPI France[2], and supported by the Committee for the Security Industrial Sector, an agency under the tutelage of the Prime Minister's office[3] (Allix 2018; BPI France 2018)

The first facial recognition test of the Safe city project took place from 16 February to 2 March 2019, during the Nice Carnival. The experiment was a simulation, involving matching faces collected through CCTV footage of the crowd attending the carnival with a fictitious set of databases (lost individuals, wanted individuals, or individuals with restraining orders). The fictitious datasets were constituted by 50 volunteers, recruited mostly among the municipality, who provided their pictures, or were freshly photographed for the test. The system used live facial recognition software provided by the company Anyvision. The live feeds were filmed during the carnival. Passers-by (approximately 1000 people were concerned) were informed of the ongoing test and asked to wear a bracelet if they consented to being filmed (Hassani 2019).

A second experiment took the form of a software application (app) named "Reporty", rolled out in January 2018. The app, developed by the Israeli American company Carbyne, allows citizens to be in direct audio and video connection and share geolocation information with the Urban Supervision Centre in order to report any incivility, offense, or crime that they might witness (Barelli 2018).

1 The other companies are: Arclan Systems, Business Card Associates, Deveryware, Egidium, Gemalto, Geol Semantics, Igo, Inria, Luceor, Onhys, Idemia, Sys, Sysnav and Yncrea.

2 Banque Publique d'Investissement: French Public Investment Bank

3 Comité de la Filière industrielle de la sécurité

The third project, involving facial recognition was tested in the education context. In February 2019, a high school in Nice and a high school in Marseille were fitted with facial recognition technology at their gates in order to grant or bar access to the premises. The official motivation behind the deployment was to "assist the personnel of the high schools and to fight against identity theft'' (Dudebout 2020, 3–4).

LEGAL BASES AND CHALLENGES

The use of facial recognition systems in high schools in Nice and Marseille, which was declared unlawful by the Administrative Court of Marseille, raised important issues on the legality of deploying biometric technologies in public places.

There is no specific provision devoted to the right to privacy or data protection in the French Constitution of 1958, but constitutional safeguards for the interests protected under said rights exists. The French Constitutional Council (Conseil Constitutionnel) has recognised that the respect for privacy is protected by Article 2 of the 1789 Declaration of the Rights of Man and of the Citizen, which is incorporated in the French constitutionality bloc as binding constitutional rule (bloc de constitutionnalité) (French Constitutional Council, Decision N° 2004-492 DC of 2 March 2004). Accordingly, the collection, retention, use and sharing of personal data attracts protection under the right to privacy (French Constitutional Council, Decision n° 2012-652 DC of 22 March 2012). The limitations to that right must thus be justified on grounds of general interest and implemented in an adequate manner, proportionate to this objective (ibid).

France has updated the Act N°78-17 of 6 January 1978 on information technology, data files and civil liberties in various stages to incorporate the provisions of the GDPR, address the possible exemptions contained in the GDPR, and implement the LED.

The Act sets out the reserved framework for sensitive data including biometric data in its Article 6, which states that sensitive data can be processed for purposes listed in Article 9(2) of the GDPR as well as those listed in its Article 44. The latter includes the re-use of information contained in court rulings and decisions, provided that neither the purpose nor the outcome of such processing is the re-identification of the data subjects; and the processing of biometric data by employers or administrative bodies if it is strictly necessary to control access to workplaces, equipment, and applications used by employees, agents, trainees, or service providers in their assignments.

Pursuant to Article 6 of the Act N°78-17, processing of sensitive data can be justified for public interest if it is duly authorised in accordance with Articles 31 and 32 of the Act. Accordingly, an authorisation by decree of the Conseil d'État (State Council) is required after reasoned opinion of CNIL, for processing of biometric data on behalf of the State for the authentication of control of the identity of the individuals (Article 32, Act N°78-17).

In February 2020, the Administrative Court of Marseille considered the extent to which the data subject's explicit consent may provide an appropriate legal basis in the deployment of facial recognition systems to control access to high schools in Nice and Marseille (Administrative Court of Marseille, Decision N°1901249 of 27 February 2020). After recognising that data collected by facial recognition constitute biometric data (para 10), the Court held that the required consent could not be obtained simply by the students or their legal representatives in the case of minors signing a form due to the power imbalance between the targeted public and the public educational establish-

ment as the public authority (para. 12). More importantly, the Court determined that the biometric data processing could not be justified based on a substantial public interest (i.e., controlling access to premises) envisioned in Article 9(2)(g) of the GDPR in the absence of considerations that the relevant aim could not be achieved by badge checks combined with – where appropriate – video surveillance (ibid).

Article 88 of the Act N°78-17 provides the specific limitations of the processing of sensitive data for law enforcement purposes, according to which their processing is prohibited unless it is strictly necessary, subject to appropriate safeguards for the data subject's rights and freedoms and based on any of the same three grounds listed in Article 10 of the LED, including where it is authorised by law.

The Act N°78-17 provides the data subject rights against the processing of their personal data with restrictions to the exercise of those rights subject to certain conditions (e.g., the restriction for protecting public security to the right to access the data processed for law enforcement purposes pursuant to Art 107 of Act N°78-17). An important data subject's right in the context of biometric surveillance is the data subject's right not to be subjected to solely automated decision-making, including profiling, except if it is carried out in light of circumstances laid out in Article 22 of the GDPR and for individual administrative decisions taken in compliance with French legislation (Article 47 of Act N°78-17). That said, for the latter circumstance, the automated data processing must not involve sensitive data (Article 47(2), Act N°78-17). Regarding the data processing operations relating to State security and defence (Article 120, Act N°78-17) and to the prevention, investigation, and prosecution of criminal offences (Article 95, Act N°78-17), the Act lays out an absolute prohibition against solely automated decision-making, according to which no decision producing legal effects or similarly significant effects can be based on said decision-making intended to predict or assess certain personal aspects of the person concerned. Particularly, with respect to data processing operations for law enforcement purposes, Article 95 of the Act prohibits any type of profiling that discriminates against natural persons based on sensitive data as laid out in Article 6.

In addition to the data protection legislation, the other legislation applicable to biometric surveillance is the Code of Criminal Procedure. Its Article R40-26 allows the national police and gendarmerie to retain in a criminal records database (Traitement des Antécédents Judiciaires or TAJ) photographs of people suspected of having participated in criminal offences as well as victims and persons being investigated for causes of death, serious injury or disappearance to make it possible to use a facial recognition device. According to a 2018 report by Parliament, TAJ contains between 7 and 8 million facial images (Assemblée Nationale N°1335, 2018, 64, f.n. 2). La Quadrature du Net lodged legal complaints against the retention of facial images before the Conseil d'État, arguing that this practice does not comply with the strict necessity test required under Article 10 of LED and Article 88 of Act N°78-17 (La Quadrature du Net, 2020).

MOBILISATIONS AND CONTESTATIONS

The political agenda of Nice's mayor to be at the forefront of biometric mass surveillance technologies in France and possibly in Europe has put him on a collision course with two main actors: the French Data Protection Authority (CNIL) and human rights/digital rights organisations.

The French digital rights organisation La Quadrature du Net was quick to highlight the problems raised by the deployment of these

technologies in Nice. “The safe city is the proliferation of tools from the intelligence community, with a logic of massive surveillance, identification of weak signals and suspicious behaviour," commented Félix Tréguer, a Marseilles-based leader of the association La Quadrature du Net and member of the campaign Technopolice[4]. “We do not find it reassuring that the municipal police will become the intelligence service of the urban public space and its digital double" (Allix 2018).

The Ligue des Droits de l’Homme emphasised similar points, highlighting the political dangers involved. As Henri Busquet of the Ligue des Droits de l'Homme in Nice put “improving emergency services and traffic is legitimate, but the generalisation of video surveillance worries us, and scrutinising social networks is not the role of a mayor. Without any safeguards, such a tool cannot demonstrate the necessary neutrality [...] It is potentially a tool for political destruction, which puts opponents and journalists at particular risk” (Allix 2018).

In July 2019, the city of Nice hoped the CNIL would provide advice related to its first test experiment during the Carnival. The CNIL responded however that not enough information was provided by the municipality for the DPA to assess it. The French DPA pointed out in particular the lack of “quantified elements on the effectiveness of the technical device or the concrete consequences of a possible bias (related to gender, skin colour ...) of the software” (Dudebout 2020, 3).
The launch of the smartphone application “Reporty” was the catalyst for mobilisation in Nice, united under the umbrella organisation “Collectif anti-Reporty". The coalition was formed by local representatives from two left-wing parties (Parti Socialiste, Les Insoumis), Tous Citoyens, the union CGT and the anti-discrimination NGO MRAP. The coalition appealed to two institutions to block the use of the application: The Defender of Rights (Défenseur des Droits) and the French DPA (CNIL). The coalition denounced “a risk of generalised denunciation and a serious breach of privacy”, calling to “put an end to the securitarian drift of Christian Estrosi” (Barelli 2018).

On 15 March 2018, the CNIL stated that the application was too invasive and did not meet the criteria set out by the legislation. It did not meet the proportionality test; it failed to fall within the frame of existing law on video-protection due to the integration of private citizens terminals (smartphones) with a security database managed by the police; it was excessively intrusive due to the collection of images and voice of people in the public space and finally it covered a field of offenses that was too broad (CNIL 2018).

The school experimentation further pushed the CNIL to take a position on the technological activism of Nice’s mayor. On 29 October 2019, it expressed serious concerns over the experimentation, arguing that the technology was clashing with the principles of proportionality and data collection minimisation enshrined in the principles of the GDPR. It pointed out that other methods, less intrusive for the privacy of the students, could be used to achieve the technology’s stated goal, namely increasing the student’s security and traffic fluidity (Dudebout 2020, 4).
In a landmark opinion published on 15 November 2019, the CNIL clarified what it defined as guidelines related to facial recognition (CNIL 2019a). The French DPA expressed concerns over a blanket and indiscriminate use of the technologies, highlighting possible infringements to fundamental rights, because these technologies operate in the public space, where these freedoms (expression, reunion, protest) are expressed. It however did not sug-

4 For the campaign, see: http://www.technopolice.fr

gest that they should be banned in all circumstances – it suggested instead that its uses could be justified if properly regulated, on a case-by-case basis. Certain uses could be rejected a priori – such as in the case of minors, whose data are strictly protected. The question of data retention is also central, warning against excessive data duration and excessive centralisation, suggesting instead citizen's control over their own data. But as the president of the CNIL, Marie-Laure Denis explained, facial recognition technology "can have legitimate uses, and there is a not firm position of the CNIL's board" (Untersinger 2019).

The repeated rebukes of the Nice's experimentation with facial recognition technology by the CNIL have however not tempered the enthusiasm of the mayor. Rather than cave in, Estrosi questioned the legitimacy of the CNIL's decisions, arguing that the legal framework, and in particular the French law of 1978 regulating data collection in relation to digital technologies was itself a limitation. In 2018, Estrosi asked: "I have the software that would allow us to apply facial recognition tomorrow morning and to identify registered individuals wherever they are in the city... Why should we prevent this? Do we want to take the risk of seeing people die in the name of individual freedoms, when we have the technology that would allow us to avoid it?" (Allix 2018) In December 2019, Estrosi reiterated his attacks on the CNIL, and together with the mayor of Gravelines Bertrand Ringot (Socialist Party) accused the institution of acting as a "permanent obstruction to the development of digital experiments" (Dudebout 2020, 5).

EFFECTS OF THE TECHNOLOGIES

To our knowledge, there has not been any systematic ex-post impact assessment of the effects of these three experiments in the city of Nice.

The city of Nice asked the CNIL to provide an assessment of the Carnival experiment, but the CNIL refused to do so, arguing that not enough information had been communicated to them about the parameters of the experiment.

There are no systematic qualitative or quantitative studies about the perception of the citizens in relation to the technologies in Nice. While the political opposition to these technologies has been documented, it would be erroneous to conclude that they are generally unpopular among the population. Surveys conducted at the national level, such as the one carried out by the organisation Renaissance Numérique show that the public is generally supportive. While 51% of the polled citizens consider that the technologies are not transparent, do not sufficiently allow for consent and can potentially lead to mass surveillance, 84% consider it justified for National Security issues (kidnappings, terror attacks), 76% to secure important public events, and 72% consider it justified to secure public spaces in general. Only when asked about their faith in private actors using the technologies properly, the confidence rates decline (38%). (Reconnaissance Numérique 2019)).

As one press article reports, "For their part, many people in Nice do not seem to be hostile to this application". The article further quotes a 72-year-old from Nice: "With terrorism, any measure that allows us to reinforce security seems desirable to me. On the condition that we don't give this application to just anyone". (Barelli 2018)

CHAPTER 9

FACIAL RECOGNITION IN HAMBURG, MANNHEIM & BERLIN

(GERMANY)

FACIAL RECOGNITION IN HAMBURG, MANNHEIM & BERLIN (GERMANY)

Key points

- The German federal police, in cooperation with the German railway company, conducted a project called “Sicherheitsbahnhof” at the Berlin railway station Südkreuz in 2017/18, which included 77 video cameras and a video management system.
- The police in Hamburg used facial recognition software Videmo 360 during the protests against the G20 summit in 2017. The database includes 100.000 individuals in Hamburg during the G20 summit and whose profiles are saved in the police database. The technology allows for the determination of behaviour, participation in gatherings, preferences, and religious or political engagement
- Sixty-eight cameras were installed by local police on central squares and places in the German city Mannheim to record the patterns of movement of people. In this project, which started in 2018, the software is used to detect conspicuous behaviour.
- Half of these deployments (Mannheim & Berlin Südkreuz) took place as measures to test the effectiveness of facial recognition and behavioural analysis software. This “justification as a test” approach is often used in Germany to argue for a deviation from existing rules and societal expectations and was similarly applied during deviations to commonly agreed measures in the Coronavirus/COVID-19 pandemic.
- Resistance to video surveillance is also in no small part a result of constant campaigning and protest by German civil society. The Chaos Computer Club and Digital Courage have consistently campaigned against video surveillance and any form of biometric or behavioural surveillance. The long term effect of these “pilots” is to normalise surveillance.

RBI DEPLOYMENTS IN GERMANY

All the deployments of RBI we are aware of in Germany were conducted by law enforcement. The deployments range from using facial recognition software to analyse the German central criminal information system, to specific deployments in more targeted locations such as Berlin Südkreuz train station or Mannheim city centre, or to deployments around specific events such as the G20 in Hamburg in 2019.

Pilot Project Südkreuz Berlin

The German federal police (BPOL), in cooperation with the Deutsche Bahn AG, the German railway company, conducted a project called "Sicherheitsbahnhof" at the Berlin railway station Südkreuz in 2017/18. The project consisted of two parts: part one was done from August 2017 until January 2018 with 312 voluntary participants. Part two was carried out from February until July 2018, including 201 participants (Bundespolizeipräsidium Potsdam 2018).

For the first project, 77 video cameras and a video management system were installed at the train station Berlin Südkreuz. Three cameras were used for the biometric facial recognition during live monitoring. During the project, the systems BioSurveillance by the company Herta Security, delivered by Dell EMC AG, Morpho Video Investigator (MVI) by IDEMIA AG, and AnyVision by Anyvision were used and tested. To detect and identify faces, the systems worked based on neural networks using Template Matching Methods. For that purpose, images of the faces were recorded and converted into templates. Subsequently, the facial recognition software matched the unknown picture to a known model saved in the reference database. As soon as a certain threshold of similarity is reached, the image is considered a match (see 2.3. for a technical description) The reference database consisted of high-quality images of the participants. That means the photographs had to adhere to quality standards such as a neutral grey background, no shadow in the faces, enough lighting, low compression to avoid artefacts, high resolution, and a straightforward viewing direction (Bundespolizeipräsidium Potsdam 2018).

For the first testing phase, the participants passed the designated area of the train station Berlin Südkreuz a total of 41.000 times. BioSurveillance had an average hit rate of 68,5%, MVI of 31,7%, and AnyVision 63,1%. A combined hit rate by the interconnection of the three systems resulted in an increased total hit rate of 84,9%. The interconnection also increased the rate of false positives. The matches were logged but not saved (Bundespolizeipräsidium Potsdam 2018).

For the second testing phase, the reference database consisted of participant images from the video stream of the first testing phase. For each participant, 2-5 images were extracted from the video stream. The images recorded during the second testing phase generally were of worse quality than from the first phase. All systems used more than one picture as a reference to identify a person (Bundespolizeipräsidium Potsdam 2018). During the second phase, the interconnected systems had an average testing rate of 91,2%. BioSurveillance resulted in an average hit rate of 82,8%, MVI in 31,2%, and AnyVision in 76,2%. The performance increased as the systems had more images as a reference (Bundespolizeipräsidium Potsdam 2018).

The Deutsche Bahn AG used the existing infrastructure at the railway station Berlin Südkreuz for an experiment on behavioural analysis starting in June 2019. The tests were done twice a week during the day. Volunteers performed situations the system should recognise and identify. After scanning people's behaviour, the software would alert the police or

the railway company (Henning 2019). The police assembled a list of behaviours that should be recognised by the system: people lying down or entering certain zones of the train station (such as construction areas), groups of people or streams of people, objects that were set down such as luggage, and the positions of persons and objects. Furthermore, the system would be counting the number of people in certain areas and allow the analysis of the video data by the police. The software used by the tests is provided by IBM Germany GmbH, the Hitachi Consortium (Hitachi, Conef, MIG), Funkwerk video systems GmbH and G2K Group GmbH (Bundespolizei 2019).

Hamburg G20 Summit

The police in Hamburg used facial recognition software Videmo 360 (by Videmo) during the protests against the G20 summit in 2017 (Bröckling 2019). The database, consisting of 100 TB of data, consists of material the police assembled during recording identities in investigations and data from external sources such as surveillance cameras in train stations, the BKA's online portal called "Boston Infrastruktur", from the internet and the media. "Boston Infrastruktur" is a web portal accessible to the public in July 2017, where people could upload images and videos. All data that concerns the time and place of the G20 summit were included.

Furthermore, data were assembled in 2017 during investigations of the special commission "Schwarzer Block" in the context of the G20 summit protests. The images were first detected and identified, meaning templates of faces were made. Subsequently, experts checked the material manually (Caspar 2018). The database includes 100.000 individuals in Hamburg during the G20 summit and whose profiles are saved in the police database. The technology allows for the determination of behaviour, participation in gatherings, preferences, and religious or political engagement (Bröckling 2019).

Mannheim public surveillance

68 cameras were installed by local police on central squares and places in the German city Mannheim to record the moving patterns of people. In this project, which started in 2018, the software developed by the Fraunhofer Institute of Optronics in Karlsruhe is used to detect conspicuous behaviour. The police are alerted by the cameras and investigate the emerging situation they have observed on camera further (Reuter 2018). The cameras were placed in areas with increased incidences of criminal activity. Only two minutes lie between the alert of the system and the intervention by the police on average. As the software is learning, it is increasingly able to detect criminal or violent activity. However, sometimes the alerts are not correct, for instance, the system cannot recognise a hug as not dangerous (heise online 2020). The software is continuously tested and adapted to be suitable for public spaces. Twenty cameras are used to test the software (Ministerium für Inneres 2020).

LEGAL BASES AND CHALLENGES

The question on the legal permissibility of examples of biometric video surveillance explained above requires a brief description of the constitutional and legislative framework for the protection of privacy and personal data, and the police powers granted under the German law in relation to the use and processing of personal data.

The general right of personality based on Articles 2(1) and 1(1) of the German Constitution protects individuals against the collection, storage, and use of their personal data by public authorities (Eichenhofer and Gusy, 2017). The basic right to informational self-de-

termination guarantees the authority to decide on the disclosure and also on the type of use of one's personal data (BVerfG, judgment of 15 December 1983 - 1 BvR 209/83, para. 149).

Germany adapted a new Federal Data Protection Act (BDSG), to use the discretionary powers and the application of national laws contained in the GDPR. The BDSG also contains data protection provisions on the processing of personal data by activities of public federal bodies which do not fall within the scope of Union law (e.g., intelligence services, Federal Armed Forces) (Part 4, BDSG) and implements the LED (Part 3, BDSG).

Paragraph 22 of the BDSG sets out lawful purposes additional to those listed in Article 9 of the GDPR for which sensitive data may be processed. For the purpose of this report, the lawful purposes that are relevant for public bodies processing operations are the following: (i) processing is urgently necessary for reasons of substantial public interest; (ii) processing is necessary to prevent substantial threats to public security; (iii) processing is urgently necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good; (iv) processing is necessary for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body. In each case, the interests sought with any of these purposes must outweigh the data subject's interest. Paragraph 22 of the BDSG further imposes obligations such as access restriction and encryption in relation to implementing appropriate safeguards to protect the data subjects' interest when the processing is carried out based on the above purposes. Furthermore §27 of the BDSG envisages the processing of sensitive data for scientific or historical research purposes or statistical purposes subject to certain conditions.

In regard to the processing of sensitive data for law enforcement purposes, §48 of the BDSG permits the processing only where it is strictly necessary for the performance of the competent authority's task, and subject to the existence of certain safeguards such as those in relation to data security and encryption.

In terms of the further use of the data, §23 of the BDSG designates purposes for which personal data may be processed other than the initial intended purpose such as where it is necessary to prevent substantial harm to common good, threat to public security, defence, or national security or where it is necessary to prevent serious harms to others' rights. §49 of the BDSG lays out the rules for the processing of personal data for law-enforcement purposes other than the initial intended law enforcement purpose.

Moreover, the BDSG devotes a specific section to the processing of personal data while conducting video surveillance. Pursuant to §4 of the BDSG, video surveillance of public spaces is permitted only as far as it is necessary (i) for public bodies to perform their tasks; (ii) to exercise the right to determine who shall be allowed or denied access, or (iii) to safeguard legitimate interests for specifically defined purposes. There should be nothing to indicate that the data subject's legitimate interest overrides the interest protected by any of the respective purposes and protecting lives, health and freedom of people should be considered as a very important interest (§4, the BDSG). More importantly, the data collected through the use of video surveillance can be further processed if it is necessary to prevent threats to state and public security and to prosecute crimes (§4(4), the BDSG). The same section further provides conditions for notification at the earliest possible moment about the surveillance, informing the data subject

whose personal data may be collected as a result of the surveillance and the deletion of the data if it is no longer necessary.

The BDSG restricts the application of certain data subject rights as enshrined in the GDPR such as the right to be informed (§33) and the right to request access (§34). §37 of the Act provides a sectorial exception in relation to providing services pursuant to an insurance contract for the prohibition against the sole automated decision-making. In relation to the processing of personal data for law enforcement purposes, the BDSG permits the sole automated decision-making if it is authorised by law (§55). Nevertheless, the decision cannot be based on sensitive data unless there are suitable safeguards to the data subject (§55(2)). In any case, it provides an explicit prohibition against conducting profiling that may discriminate against people based on their sensitive data (§55(3)).

The collection of personal data in general and facial images in particular in criminal investigation proceedings are authorised under German Law by the Federal Police Act (Gesetz über die Bundespolizei) (BPolG), by the Federal Criminal Police Office and the Cooperation of the Federal and State Governments in Criminal Police Matters (Bundeskriminalamtgesetz) (BKAG), the Code of Criminal Procedure (Strafprozessordnung) (StPO), and the police acts of Länder.

§24 of the BPolG grants the Federal Police the authority to take photographs including image recordings of a person subject to specific conditions. Moreover, §26 of the BPolG, entrusts the Federal Police the power to collect personal data by making picture and sound recordings of participants in public events or gatherings if facts justify that there are significant risks to border security or to categories of people or objects. §27 of the BPolG further authorises the use of automatic image recording, albeit in relation to security risks at the border or to categories of people or objects. Each section provides the obligations for the deletion of the data after a specific timeframe.

The BKAG provides the rules for information collection by the Federal Criminal Police Office in its information system, BKAG established pursuant to §13 of the BKAG. §12 of the Act allows the processing of personal data by the Office for purposes other than those for which they were collected in order to prevent, investigate, and prosecute serious crimes. Additionally, the personal data of people who are convicted of, accused of, and suspected of committing a crime, and for whom there are factual indications that they may commit crimes of considerable importance in the near future may be processed to identify that person. (§12, para. 5, the BKAG). The same Article states that personal data obtained by taking photos or image recordings of a person by means of covert use of technical means in or out of homes may not be further processed for law enforcement purposes.

§81b of the StPO grants the police the authority to obtain the photographs and fingerprints of a suspect and any of his measurements in order to conduct criminal proceedings. §100h of the StPO covers the police power to conduct covert surveillance measures, which includes the recording of the photographs and other images of the person concerned outside of private premises where other means of establishing the facts or determining an accused's whereabouts would offer less prospect of success or would be more difficult. In terms of the investigative powers of police to use personal data in general, §98c of the StPO grants the authority to automatic matching of personal data from criminal proceedings with other data stored for the purposes of criminal prosecution or the enforcement of a sentence,

or in order to avert a danger. This is, however, subject to the specific rules under federal law or Länder law. §483 of the StPO authorises a number of authorities to process personal data where necessary for the purposes of criminal proceedings including for criminal proceedings other than the one for which the data were collected. §484 of the StPO allows for the processing of personal data for future criminal proceedings.

MOBILISATIONS AND CONTESTATIONS

What is notable about these deployments, is that two thirds of them (Mannheim & Berlin Südkreuz) took place as measures to test the effectiveness of facial recognition and behavioural analysis software. This "justification as a test" approach is often used in Germany to argue for a deviation from existing rules and societal expectations and was similarly applied during deviations to commonly agreed measures in the Coronavirus/COVID-19 pandemic. Similar special justifications were used for biometric surveillance around the G20 in Hamburg, which was justified by referencing the exceptional security threats associated with these large summits. Thus, three out of four implementations of biometric or behavioural surveillance in Germany - and all of those in Germany using video data - require special justifications in order to be able to take place at all. Notably, German civil society such as the Chaos Computer Club - a central civil society watchdog promoting fundamental rights in the digital age - have criticised these "tests" as not being very scientific in nature (Chaos Computer Club 2018).

The Berlin experiments were criticised as being unscientific in the handling of the data, the low number of participants and the use of pictures of high quality in the database. Moreover, the Chaos Computer Club asserted that the results would not justify using the technology on a bigger scale as it did not function very well due to its low hit rate (Chaos Computer Club 2018). The fact that such special justifications are even needed in order to conduct biometric or behavioural surveillance in Germany, suggests that it is highly unpopular in society. Both the German public and civil society have argued strongly against all forms of video surveillance, which is itself already uncommon compared to many other places in Europe. In this context, biometric or behavioural surveillance has been very difficult to justify. Even when behavioural surveillance projects receive approval from data protection authorities (Wazulin 2019a), these projects are still criticised for not taking privacy sufficiently seriously (Wazulin 2019b).

However outside of Mannheim, German DPAs have been one of the central actors contesting biometric and behavioural video surveillance. Once given the opportunity to analyse the usage of biometric video surveillance during the G20, the Hamburg data protection authority (Hamburgische Beauftragte für Datenschutz und Informationsfreiheit) found this use to be in breach of data protection laws (Schemm 2018). It considered that the StPO did not provide the legal basis to authorise that surveillance on the basis that the facial recognition technology took place independently of the initiation of a specific investigation (DPA Hamburg, 12). The Hamburg DPA further argued that §98c of the StPO did not provide the legal basis for authorisation because it covers only the comparing of the data and assumes the legality of the other data processing cycle (e.g., collection and storage). A criminal suspicion is not a pre-requisite to conduct the comparison, and, on that basis, the Hamburg DPA argued that it authorised only minor interferences with fundamental rights (25). Along those arguments on the legality of the biometric video surveillance at the G20 summit, the Hamburg DPA ordered the database of data collected by the police during that surveillance to be dele-

ted (Caspar 2018) but were unsuccessful in a legal battle with the Hamburg police to compel them to delete the database (Bröckling 2019).

Resistance against video surveillance is also in no small part a result of constant campaigning and protest by German civil society. The Chaos Computer Club and Digital Courage have consistently campaigned against video surveillance and any form of biometric or behavioural surveillance. The widely popular online blog Netzpolitik.org has also reported extensively on video surveillance technologies, as have other leading German media outlets like Sueddeutsche Zeitung or Die Zeit. As a result, it is difficult to implement biometric or behavioural surveillance in Germany without being noticed by civil society and engaging in a public debate about whether these forms of surveillance are appropriate. Therefore, biometric, or behavioural surveillance can only be found in a limited set of cases in Germany, for which purported tests or exceptional justifications are typically required.

EFFECTS OF THE TECHNOLOGIES: NORMALISING SURVEILLANCE

As there have only been a few implementations of behavioural or biometric surveillance in Germany, many of which have been as part of tests or for "exceptional circumstances", their effects are relatively hard to measure. In some cases this can lead to a normalisation of video surveillance, as was the case in Hamburg (Gröhn 2017). The video surveillance cameras that were installed for the G20 summit remain in use and additional video surveillance cameras have since been installed.
All of the video data stored by the Hamburg police during the G20 remains stored by the police and even if the Hamburg data protection authority believes that it should be removed, deletion is not currently possible. This video data includes several days of footage from central Hamburg from 6-10 July 2017 and includes many people going about their daily lives without any indication of committing a crime (Monroy 2018).

Another element of normalisation is in regard to the integration of biometric facial recognition for historical data using the German central criminal information system INPOL. Historical data of the usage of the systems shows a systematic year on year increase in the number of requests being made to the system by the German police (Monroy 2020), even though the number of criminal offenses has gone down steadily over the past decade (Statista 2021).

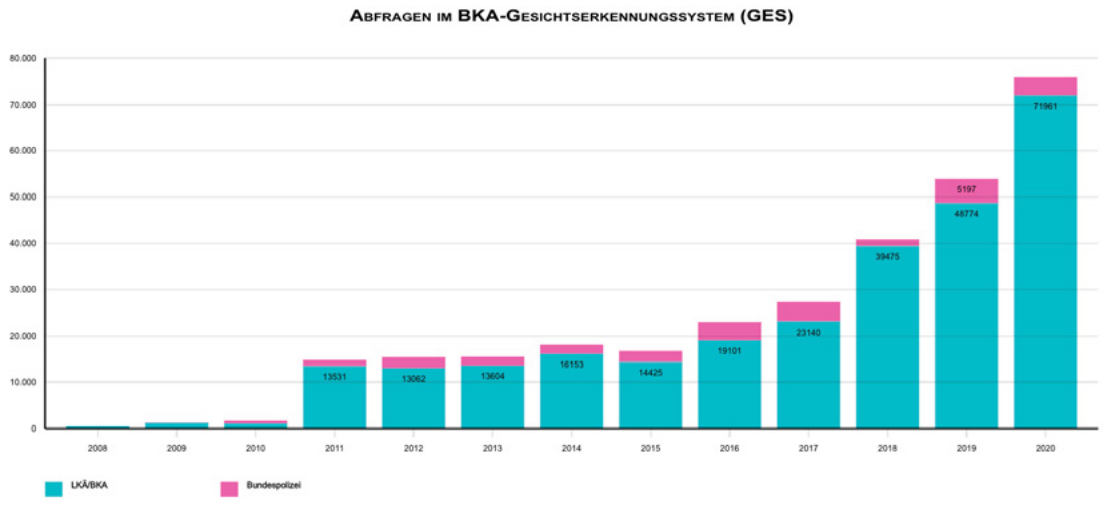


Figure 4. *Growth in police requests to INPOL system*[1]

1 Image from https://netzpolitik.org/2020/deutlich-mehr-gesichtserkennung-bei-bundespolizei-und-kriminalaemtern/

CHAPTER 10

THE DRAGONFLY PROJECT (HUNGARY)

THE DRAGONFLY PROJECT (HUNGARY)

Key points

- The Hungarian Government led by Prime Minister Viktor Orbán has long been on a collision course with EU Institutions over the rule of law and the undermining of the country's judicial independence and democratic institutions.
- Hungary is a frontrunner in Europe when it comes to authorising law enforcement's use of Facial Recognition Technology, developing a nation-wide and centralised database (The Dragonfly Project), and using the Home Quarantine App as part of the Government's Coronavirus measures.
- The infrastructure in place that potentially allows for a centralised deployment of biometric mass surveillance technologies in Hungary has reached an unprecedented scale while the legal and ethical scrutiny of these technologies lags dangerously behind.
- This is due to (1) the overlap between the private and public sectors, specifically government institutions, and (2) the complex entanglements biometric systems have with other information systems (such as car registries, traffic management, public transport monitoring and surveillance, etc.).
- Although the latter are not concerned with the traces of the human body they can nonetheless be used for and facilitate biometric mass surveillance. These entanglements create grey zones of biometric mass surveillance where the development and deployment of such technologies is hidden from visibility and critical scrutiny.
- The Dragonfly Project has elicited numerous warnings regarding data protection and the rights to privacy from both public and private organisations. However the lack of contestation and social debate around the issues of privacy and human rights in relation to such projects as the Hungarian Government's Dragonfly is striking.

Under the Government of Prime Minister Viktor Orbán, Hungary has been on a collision course with EU Institutions. It has centralised and consolidated its power by marginalising civil society and curtailing the autonomy of Hungarian media, cultural and higher education institutions (Csaky 2020; Gehrke 2020; Verseck 2020). Orbán's continued erosion of the country's democratic institutions was further advanced with the 2020 adoption of an emergency law which allows the government to rule by decree (Schlagwein 2020; Stolton 2020). In this context, the latest developments in using Biometric Identification Technologies in Hungary flag serious concerns regarding the rule of law, human rights and civil liberties.

Hungary is a frontrunner in Europe when it comes to authorising law enforcement's use of Facial Recognition Technology, developing a nationwide and centralised database, and using the Home Quarantine App as part of the Government's Coronavirus measures. The infrastructure in place that potentially allows for a centralised deployment of biometric mass surveillance technologies in Hungary has reached an unprecedented scale while the legal and ethical scrutiny of these technologies lags dangerously behind. This is due to (1) the overlap between the private and public sectors, specifically government institutions, and (2) due to the complex entanglements biometric systems have with other information systems (such as car registries, traffic management, public transport monitoring and surveillance, etc.). Although the latter are not concerned with the traces of the human body they can nonetheless be used for and facilitate biometric mass surveillance. These entanglements create grey zones of biometric mass surveillance where the development and deployment of such technologies is hidden from visibility and critical scrutiny.

REMOTE BIOMETRIC IDENTIFICATION IN HUNGARY

The Hungarian Police's use of Facial RecognitionOn 10 December 2019 the Hungarian Parliament passed a package of amendments of acts for the work of law enforcement in Hungary. Entitled "the simplification and digitisation of some procedures" this adjustment legalised the use of forensic – but also live – FRT by the Hungarian Police (Hungarian Parliament 2019). In cases when a person identified by the police cannot present an ID document, the police agents can take a photograph of the individual on location, take fingerprints, and record the biometric data based on "perception and measurement" of external characteristics. The photo taken on location can be instantly verified against the database of the national registry of citizens. The automatic search is performed by a face recognition algorithm and the five closest matches are returned to the police agent who, based on these photos proceeds with identifying the person (1994. Évi XXXIV. Törvény, para 29/4(a)). This application of FRT does not fall under the category of mass surveillance; however, it is only possible due to a central system which collects and centralises the national and other biometric databases but also provides the technical support for accessing it in a quick and affective way by various operational units. In this instance by the patrolling police.

The Dragonfly (Szitakötő) Project

In 2018 the Ministry of Interior presented a bill in the Hungarian Government that proposed a centralised CCTV system with data stored in one centralised database called the Governmental Data Centre (Kormányzati Adatközpont, abbreviated as KAK). All governmental operations aiming at developing this centralised database run under the name Szitakötő (Dragonfly). This central storage fa-

cility collects surveillance data of public spaces (streets, squares, parks, parking facilities, etc.); the Centre for Budapest Transport (BKK); bank security and the Hungarian Public Road PLC. The project with an estimated budget of 50 billion forints (160 million euros) proposes to centralise about 35.000 CCTV cameras and 25.000 terabytes of monitoring data from across the country (NAIH 2018). While the project, and notably the response of Dr. Attila Péterfalvi, head of the Hungarian Data Protection Authority, - Hungarian National Authority for Data Protection and Freedom of Information (NAIH), who warned of the lack of data protection considerations in the bill, have been largely mediatised, this has done little for halting the Project which has already been rolled out. In 2015 the Hungarian company GVSX Ltd (Hungary). Had already been contracted (NISZ-GVSX 2019) to implement an Integrated Traffic Management and Control System called IKSZR (Integrált Közlekedésszervezési és Szabályozási Rendszer) that centralises data from various systems such as ANPR cameras, car parks, traffic monitoring, meteorological data, etc. The Dragonfly Project has been designed as an expansion of this system by centralising the data flowing from both the IKSZR system, the databases of the National Infocommunication Services (NISZ) and also CCTV data from other public and private surveillance systems such as those operated by local governments, public transport companies and banks.

The technical description of the Dragonfly Project does not make any explicit reference to (live) facial recognition technology, however, the system collects, stores and searches, in real time, video surveillance footage from 35.000 CCTV cameras. However, from the reports of the Hungarian Civil Liberties Union (HCLU or TASZ in Hungarian) and the DPA, it is known (NAIH 2019, 139) that to some extend FRT has been used by the Secret Service for National Security (SSNS), one of the national security services of Hungary. According to the DPA's investigation all the cases in which FRT has been used happened in relation to concrete (criminal) cases looking for a missing person or someone under warrant. These cases were also limited to specific geographic locations (NAIH 2019). According to the DPA's investigation, in 2019 the FRT system operated by the SSNS found 6.000 matches, which resulted in around 250 instances of stop-and-search and 4 arrests (NAIH 2019). The numbers for 2020 are inconsistent with those given for 2019 (3 matches, 28 instances of stop-and-search, unknown number of arrests), however, this is probably due to the fact that the system has since been moved primarily to the jurisdiction of the Hungarian Police.

While the legal framework for police checks does refer to the use of facial recognition technologies, the national security act does not mention it. This is even more striking as the SSNS, is known to be using FRT to provide the national security services, the police, or other authorised institutions (e.g., prosecutor's office, tax office, etc.) classified information.

Two interrelated companies are responsible for the development, maintenance, and administration of this single central system: the NISZ and IdomSoft Ltd., both owned by the state. The NISZ or National Infocommunication Services is a 100% state owned company that only in 2020 signed 6 contracts to purchase the necessary hardware, storage, and other IT equipment for implementing the Dragonfly Project. While Public Procurement documents (Közbeszerzési Hatóság, 2020) bear witness to the ongoing investments and development of the Dragonfly Project by the Hungarian

Government, a comprehensive overview of the project, the stages of its implementation or its budget, is nowhere to be found.

The other company responsible for the administration of the Dragonfly Project is the IdomSoft company, a member of the so called NISZ group. Idomsoft is a 100% indirect state-owned company (indirect ownership means that the government owns shares, but not through authorised state institutions or through other organisations) that, according to its website, "plays a leading role in the development, integration, installation and operation of IT systems of national importance". Apart from administering the National Dragonfly Database, Idomsoft also assures the interoperability of the various national databases such as the citizen's registry, passport and visa databases, car registries, and police alerts, and it connects the Hungarian databases into the Schengen Information System (SIS II).

Since the implementation of the Dragonfly Project the Hungarian government has been collecting video surveillance data that is centralised in the Governmental Data Centre (Kormányzati Adatközpont) in the same location and by the same institutions that administer the national registry of citizens, visa-entries, police databases, and also other e-governmental databases such as related to social security, tax office or health records.

While the COVID-19 pandemic has brought a temporary halt of movement in public spaces, it also facilitated the introduction of new tracking technologies. Hungary is among two countries in Europe (Poland being the other) to introduce a Home Quarantine App which uses automated face recognition technology to verify that people stay in quarantine for the required time.

The normalisation of biometric surveillance at home: The Hungarian Home Quarantine App

In May 2020 Hungarian Authorities rolled out two digital applications, the contract-tracing app called VirusRadar (Kaszás 2020) and the Home Quarantine App (Házi Karantén Rendszer, abreviated HKR). Both of these apps are centralised tracing apps meaning that they send contact logs with pseudonymised personal data to a central (government) back-end server (Council of Europe 2020, 28). While the VirusRadar only uses Bluetooth data and proximity of other devices, the HKR processes biometric data when comparing facial images of its users.

Those who, according to the COVID-19 regulations in Hungary, are confined to home quarantine are offered the option to use the app instead of being checked by the police. For those who return from abroad, the use of the app is compulsory. But even those who can choose are encourage by the authorities to make use of the HKR app otherwise they will be subjected to frequent visits by police agents. Once a person downloads the app, its use becomes compulsory and failure to do so or attempts to evade its tracking is considered an administrative offense. From a data protection law point of view, this is a clear case where the data subject's consent (and in the case of biometric data, their explicit consent) cannot provide the lawful ground for the processing of data through the app (see section 4.2.2). Even if the processing can be based on another lawful ground such as public interest, the punitive nature of non-compliance may raise issues in terms of adhering to the ne-

cessity test, which requires a balancing act between the objective pursued and the data subject's interests.

The HKR app is developed by Asura Technologies and implemented by IdomSoft Ltd., the same company that provides the software and technical implementation for the nation-wide Dragonfly Project. The HKR application works with face recognition technology combined with location verification. The application sends notifications at random times prompting the user to upload a facial image while retrieving the location data of the mobile device. The user must respond within 15 minutes and the location data must match the address registered for quarantine. In order for the Home Quarantine App to work, the user first

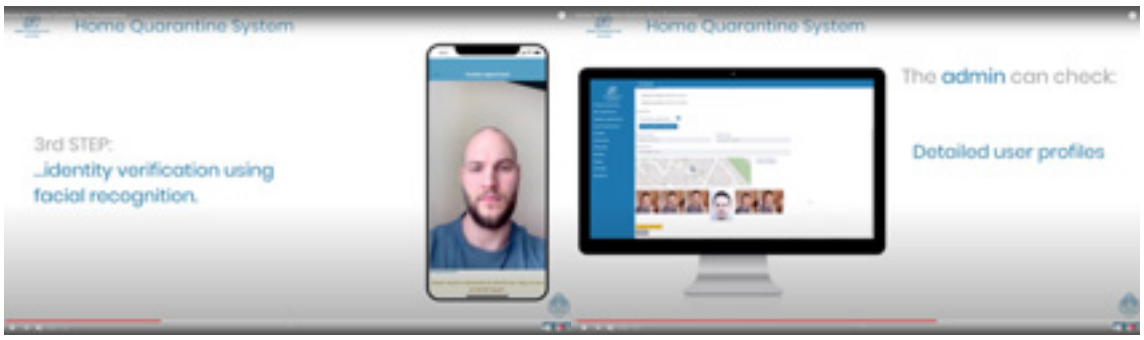


Figure 4. *Growth in police requests to INPOL system*[1]

1 https://youtu.be/5WD9b6tWC0Q

needs to upload a facial image which is compared by a police officer with the photo of the same individual stored in the central database. After this facial verification, the app creates a biometric template on the mobile phone of the user and the photo is deleted. The consecutive photos are only compared to this biometric template, so neither the photos nor the template leave the personal device. If there is suspicion about the identity or whereabouts of the user, a police officer visits the address to make sure that the person is adhering to the quarantine rules.

Interestingly, the HKR app, — just like the contact tracing app VirusRadar, which was developed by Nextsense — has been "donated" to the Hungarian Government by Asura Technologies "free of charge".

LEGAL BASES AND CHALLENGES

The creation of a nation-wide and centralised database that uses facial recognition technology may raise important legal questions on its compliance under the constitutional framework and the data protection legislation. Article 6 of the Fundamental Law of Hungary affirms the right to privacy and the right to protection of personal data. They are implemented by the Right to Informational Self-Determination and Freedom of Information (2011. évi CXII. Törvény az információs önrendelkezési jogról és az információszabadságról) (Infotv), which was amended in 2018 to use the discretionary powers and application of national laws contained in the GDPR. With the amendments, the Act also provides rules for the data processing activities that fall outside the scope of the GDPR and implements the LED. The sectoral laws on the processing of personal data have been amended as of 2019 to comply with the GDPR.

The Infovt permits the processing of sensitive data where: (i) the processing is necessary and proportionate to protect the vital interest of the data subject or another person; (ii) the data is made publicly available by the data subject; (iii) the processing is absolutely necessary and proportionate for the implementation of an international treaty, or is required by law for the enforcement of fundamental rights, national security, prevention, detection or prosecu-

tion of criminal offences (§5). Furthermore, in relation to processing of (non-sensitive) "personal criminal data" (bűnügyi személyes adat), which is personal data obtained during criminal justice proceedings, can only be processed by state or municipal bodies for the prevention, detection and prosecution of criminal offenses and for administrative and judicial tasks, as well as criminal, civil and non-judicial matters (§5(4)).

In regard to the data subjects' rights, notably, the Infovt permits sole automated decision-making, whereby a decision based on the sole automated decision-making process may be taken if it is permitted by national law or EU law and subject to certain conditions (§6). The sole automated decision can be based on sensitive data if it is authorised by national law or EU law (§6(c)).

Recently, the Hungarian Government issued a Decree (Decree No. 179/2020 of 4 May) as a response to the COVID-19 pandemic for which it declared a "state of emergency" (Stolton 2020). The Decree restricts the scope of a number of the data subject's rights such as the right to be informed. The EDPB (2021b) was highly critical of those restrictions. It particularly considered that although the state of emergency adopted in the context of a pandemic may serve as a circumstance to trigger Article 23 of the GDPR, according to which EU Member States can restrict the scope of the data subject rights and certain data protection principles (see section 4.2.2), those states must nevertheless adhere to the guarantees enshrined in the same Article for those restrictions to be legal under the GDPR (ibid). It went further to emphasise the fundamental rights requirements that must be observed and a general blanket restriction on the scope of the data subject's rights would infringe upon the essence of fundamental rights (ibid).
In terms of the public authorities' power to use sensitive data in relation to criminal proceedings, § 269 of the Criminal Procedure Act (2017. évi XC. Törvény a büntetőeljárásró) authorises the prosecutor's office, the investigating authority, and the crime prevention, detection and counter-terrorism bodies of the police to request the existing biometric data held in accordance with the Act on the criminal registry system, the registry of judgments against Hungarian citizens passed by the courts of Member States of the European Union and the registry of criminal and police biometric data (2009. évi XLVII. Törvény a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által Magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról) and request facial image analysis from the body responsible for the management and operation of the facial image register.

The Act on Facial Image Analysis Registry and the Facial Image Analysis System (2015. évi CLXXXVIII. Törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről) creates a registry for the processing of biometric data in relation to identifications at border crossings and for law enforcement purposes (§3 and §4) and it provides a list of a number of authorities that can request facial image analysis ((§9). It is reported that the Special Service for National Security, which carries out secret surveillance operations under the National Security Services Act (1995. évi CXXV. Törvény a nemzetbiztonsági szolgálatokról), has broad powers to request data from the registry (Hidvégi and Zágoni, 2016).

As is mentioned repeatedly in this section, the Dragonfly project was introduced with legal amendments to a range of laws (see section 10.1) and was subject to criticisms by the NAIH (see section 10.3). It thus remains to be seen whether the legal basis of the project would

also satisfy the ECHR and Charter requirements.

MOBILISATIONS AND CONTESTATIONS

The Dragonfly Project has elicited numerous warnings regarding data protection and the rights to privacy from both public and private organisations (TASZ 2021). The Hungarian National Authority for Data Protection and Freedom of Information (NAIH), in October 2018 filed a communique (NAIH 2018) in which it stresses the problems raised by the centralisation and storing of visual data from as many as 35.000 CCTV cameras from all over the country and public transport facilities resulting in 25.000 terabytes of surveillance data.

The main concerns, according to the NAIH, stemmed from the fact that once the surveillance data is centralised the collecting bodies stop being the official administrators of these databases. Moreover, they won't even know how and by whom the data is collected, accessed and utilised, or for what purposes. What is even more worrisome according to this communique, is that the centralised database (Governmental Data Centre) would not administer the data either, they would only process it. Therefore, while the database can be accessed and more or less freely "used" by a number of clients (such as government organisations, law enforcement, secret services) there is no legal body who is responsible for applying the data protection measures or who would be liable in case of transgressions. Eventually the government incorporated some of the suggestions and owners of the data remain the uploading bodies to whom the requests have to be addressed for accessing the database by the different authorised bodies (e.g., the Hungarian Police).

Independent Hungarian media has also picked up the news. For instance, Hungary's leading independent economic and political weekly HVG has published an article in which they outline the bill and cite the head of the NAIH (Dercsényi 2018). Interestingly, the article starts with an announcement/amendment saying that the HVG expresses its regrets for violating the good reputation of the Ministry of Internals when claiming that the bill has not incorporated the suggestions from the NAIH, which is not true (Dercsényi 2018). However, the article still claims the opposite. Other liberal online news sites and Magazines such as the Magyar Narancs (Szalai 2019), 444.hu (Herczeg 2019) and 24.hu (Kerékgyártó 2018; Spirk 2019) also report on the case. However, the main pro-government newspapers such as Magyar Nemzet remain silent.

More recently, in January 2021, the INCLO, a network of Human Liberties NGOs published a report (INCLO 2021) in which they discuss the Hungarian Case and specifically the Dragonfly Project as an example of how the employment of FRT is at odds with the right to privacy and civil liberties. They mainly flag their concern that due to the inadequate regulation FRT can be used in conjunction with the CCTV network developed at an alarming rate.

In an interview, one of the authors of the INCLO case study, legal expert Ádám Remport, explains:

Regarding secret surveillance in general the problem is the lack of adequate supervision and an effective remedial system. The legal provisions governing national security agencies are mostly satisfactory. However, they are not necessarily enforced, or if they are breached, there's no way to find out. Not via the court — which is what our latest cases show— not via Parliament's national security committee, due to the quorum: in order for the national security committee to be operational, the majority of its members must be present. Given that the ruling Fidesz and KDNP parties hold more than half of the seats, if they decide to boycott the committee, they can prevent it from performing its job. This has already happened

on several occasions when the committee was supposed to look into surveillance cases which would potentially have been politically unfeasible for the government." (Interview by author with Ádám Remport 2021)

The lack of contestation and social debate around the issues of privacy and human rights in relations to projects such as the Hungarian Government's Dragonfly is striking. While information about the Dragonfly Project has sporadically reached the wider public any discussion of face recognition technologies employed by the HKR App has been missing.

EFFECTS OF THE TECHNOLOGIES

State operated and centralised mass surveillance systems, such as the Dragonfly Project currently under development in Hungary, bring up at least two sets of questions with regard to their societal and political effects. The first set of questions concerns visibility and the (lack of) possibility for societal debate and contestation. The second concerns the grey areas of legislations and regulations. When the development and employment of such novel technologies as biometric video surveillance and (live) facial recognition becomes entangled with the national interest of reinforcing public order, preventing terrorism, and fighting criminality, or, as with the Home Quarantine App, reinforcing Coronavirus measures, their ability to carry out effective oversight might be seriously compromised. The Hungarian Governmental Decree from 16 March 2020 is a case in point. While the decree authorises the Minister for Innovation and Technology and an operational body consisting of representatives of the Ministry of Interior, the police, and health authorities to "acquire and process any kind of personal data from private or public entities, including traffic and location data from telecommunication providers, with a very broad definition of the purpose for which the data can be used" (Council of Europe 2020, 12) at the same time ordinary courts have been suspended, thus preventing the Constitutional Court from reviewing the proportionality of measures introduced under emergency conditions (Ibid 10).

Using such technologies for the so-called public good can even attract the support of residents who want to live in safe and predictable environments. The fact that these public environments are "secured" at the expense of curtailing the human rights to privacy and to one's face and biometric data is often overlooked by the public. As the human right NGO "Hungarian Civil Liberties Union" have put it in their recent publication:

"[…] the introduction of facial recognition systems is almost never preceded by social debate. Its widespread application and the omission of public consultation can lead to the normalisation of continuous surveillance and a violation of rights, where states possess the ability of knowing where we go, whom we meet, what pubs or churches we visit" (INCLO 2021).

To bring awareness to these issues, there is a need for a strong civil society and independent media which, if seriously compromised, as in the case of Hungary, can do little to educate the general public. Talking about the lack of legal framework with regard to the use of face recognition technologies by the Hungarian Secret Services Ádám Remport explained: **"If there was oversight, I think that the use of these technologies would be probably more accepted. There's certainly a possibility for abuses. This doesn't necessarily mean that these abuses happen, first of all because it's impossible to prove them, and second, we have no direct evidence of them. This needs to be emphasised. But in reality, it only depends on the personal good will of the secret services not to breach individual's privacy rights. Because in the end there's no viable or independent oversight over their workings. They can go by the rules, and most of the times they probably do. Unless they don't. But then, we will never find out."**

CHAPTER 11

RECOMMENDATIONS

RECOMMENDATIONS

1. THE EU SHOULD PROHIBIT THE DEPLOYMENT OF BOTH INDISCRIMINATE AND "TARGETED" REMOTE BIOMETRIC AND BEHAVIOURAL IDENTIFICATION (RBI) TECHNOLOGIES IN PUBLIC SPACES (REAL-TIME RBI), AS WELL AS EX-POST IDENTIFICATION (OR FORENSIC RBI). OUR ANALYSIS SHOWS THAT BOTH PRACTICES, EVEN WHEN USED FOR "TARGETED SURVEILLANCE" AMOUNT TO MASS SURVEILLANCE.

In line with similar recommendations made by the EDPB and the EDPS,[1] the EU should prohibit the deployment of Remote Biometric and Behavioural Identification technologies in public spaces

In line with the position of the EDRi regarding's EU Artificial Intelligence Act[2], our research supports the notion that the distinction between "real-time" and "ex-post" is irrelevant when it comes to the impact of these technologies on fundamental rights. Ex-post identification carries in fact a higher potential of harm, as more data can be pooled from different sources to proceed to the identification. The use of such technologies for "targeted surveillance" is thus equally harmful as the practice might be considered as expansive and intrusive to an extent that it would constitute disproportionate interference with the rights to privacy and personal data protection.

This concerns not only the acquisition and processing of faces, but also gait, voice and other biometric or behavioural signals.

2. THE EU SHOULD STRENGTHEN TRANSPARENCY AND ACCOUNTABILITY OF BIOMETRIC AND BEHAVIOURAL RECOGNITION TECHNOLOGIES

Our research found that the majority of surveillance systems remain opaque. There is very little information on how citizens' data is processed when they enter surveilled public spaces. Rarely are concrete alternatives provided if they do not wish to be surveilled. In some extreme cases, such as the deployment of FRT trials in London, citizens who deliberately avoided surveillance by covering their faces were subjected to fines. This poses considerable challenges to citizens' rights, as well as to transparency and accountability of these systems.

It seems thus necessary to expand existing transparency and accountability requirements in the new EU Artificial Intelligence Act for biometric technologies. These requirements should be expanded to include external independent accountability, transparency and oversight for any implementations of biometric technologies that are not already prohibited by the Act.

1 https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en

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

In particular, it seems imperative to increase the transparency of such systems, by conditioning their operation to the publication of key characteristics and features (type of data acquisition, type of machine learning algorithm, nature of data collected in the database) necessary for effective public oversight of their operation. These details should be disclosed even when deployments are used for national security or law enforcement purposes, and the public should be informed about planned and ongoing projects.

3. THE EU SHOULD PROMOTE THE REINFORCEMENT OF ROBUST ACCOUNTABILITY MECHANISMS FOR BIOMETRIC SURVEILLANCE SYSTEMS

The current legislative framework remains unclear as to which institutions may review or authorise biometric surveillance systems. In light of the GDPR and the LED, the Data Protection Authorities (DPAs) in some member states enforce the relevant data protection legislation and oversee the processing of biometric data, while in others a separate authority is tasked with the responsibility to review the compatibility with the relevant legislation insofar as personal data processing by law enforcement authorities is concerned (such as Belgium, see case study).

The EU should work toward developing a centralised authorisation process for biometric surveillance, within which all relevant authorities are included and are able to veto the authorisation.

Although the proposed EU Artificial Intelligence Act limits a prior authorisation by a court or independent administrative authority to 'real-time' biometric surveillance, it is necessary to underline that ex-post biometric identification systems must be subject to supervision or authorisation taking into account the standards under the ECHR and the Charter.

4. THE EU SHOULD PROMOTE INDIVIDUAL RIGHTS UNDER THE GDPR THROUGH THE PROMOTION OF DIGITAL-RIGHTS-BY-DESIGN TECHNOLOGIES

More attention could be given to protect individuals' rights under GDPR when it comes to data collection and processing mechanisms as well as a fundamental rights assessment ex ante and ex post.

This could be implemented technically through data minimisation or digital rights-by-design methods, either through technical solutions that do not collect biometric information, or systems which incorporate automated forms of notification, immutable transparency and accountability logging, and control of data or ideally by a combination of both approaches.

5. THE EU SHOULD ENSURE EFFECTIVE ENFORCEMENT OF GDPR PURPOSE LIMITATION

Purpose limitation is one of the key principles of the GDPR. As our report shows, the re-purposing of biometric data is not always kept sufficiently in check.

From a technical perspective, biometric mass surveillance can easily emerge by connecting different elements of a technical infrastructure (video acquisition capacities, processing algorithms, biometric datasets) developed in other contexts.

For example, while the forensic use of facial recognition is not a form of remote biometric identification per se, the adoption of such systems has allowed for the creation of biometrically searchable national datasets. These datasets are one piece of a potential biometric mass surveillance infrastructure which can become a technical reality if live camera feeds, processed through live facial recognition software is connected to them.

In order to maintain democratic oversight over the uses of the infrastructure, and avoid the

risk of function creep (i.e. when a technology is being used beyond its initial purpose) it is thus imperative that the principle of purpose limitation is systematically enforced and strictly regulated with regard to the type of data (criminal or civilian datasets, datasets generated from social media, as in the Clearview AI controversy) against which biometric searches can be performed.

6. THE EU SHOULD SUPPORT VOICES AND ORGANISATIONS WHICH ARE MOBILISED FOR THE RESPECT OF EU FUNDAMENTAL RIGHTS

Our research showed that, in addition to state oversight agencies, many institutions from civil society are active in making sure that EU fundamental rights are respected in the field of biometric security technologies.

While in some countries they benefit from a dense network of civil society funding, in others they are subjected to heavy scrutiny and financial restrictions (see for example the Hungary case study in this report).

Supporting civil society organisations that operate in the sector of digital rights is therefore instrumental for a healthy democratic debate and oversight. Civil society needs to be able to participate in all relevant legislative and other decision-making procedures.

Particularly in the area of litigation, support for civil society and EU citizens access to rights could be extremely helpful. We have found numerous areas in our study where sufficient legal clarity was lacking and would likely only take place through the courts. We would thus advise that the EU support existing digital rights litigation initiatives and create additional mechanisms to support this approach.

7. THE EU SHOULD TAKE INTO ACCOUNT THE GLOBAL DIMENSION OF THE BIOMETRIC AND BEHAVIOURAL ANALYSIS TECHNOLOGY INDUSTRY

The technologies used for FRT in Europe come from vendors across the world. Technologies for biometric or behavioural analysis are often tested in one country before they are implemented in another.

EU policy on the biometric or behavioural analysis technology industry thus needs to consider its impact both inside and outside of Europe. Here, the recently revised EU Export Control framework which may include biometric and behavioural technologies can play a role.

REFERENCES

1994. Évi XXXIV. Törvény - Nemzeti Jogszabálytár. 1994. https://njt.hu/jogszabaly/1994-34-00-00.

2015. Évi CLXXXVIII. Törvény - Nemzeti Jogszabálytár. 2015. https://njt.hu/jogszabaly/2015-188-00-00.

7sur7. 2019. "Des caméras avec reconnaissance faciale à Brussels Airport." https://www.7sur7.be/belgique/des-cameras-avec-reconnaissance-faciale-a-brussels-airport-a46f7a4c/.

Access Now. 2021. 'Spotify's Speech-Recognition Patent Tech: Global Coalition Says Don't Spy'. Access Now. https://www.accessnow.org/spotify-spy-tech-coalition/ (September 29, 2021).

Access Now. 2021. "Open letter calling for a global ban on biometric recognition technologies that enable mass anddiscriminatory surveillance." https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.

Al-Kawaz, Hiba, Nathan Clarke, Steven Furnell, Fudong Li, and Abdulrahman Alruban. 2018. "Advanced Facial Recognition for Digital Forensics." In ECCWS 2018 17th European Conference on Cyber Warfare and Security V2, Oslo: Academic Conferences and publishing limited, 11-19

Algorithm Watch. 2020. Automating Society Report 2020. https://automatingsociety.algorithmwatch.org/wp-content/uploads/2020/12/Automating-Society-Report-2020.pdf

Allix, Grégoire. 2018. "Comment des villes « hyper connectées » contrôlent l'espace public." Le Monde, 19 December 2018. https://www.lemonde.fr/economie/article/2018/12/19/au-nom-de-la-smart-citydes-villes-sous-surveillance 53995273234.html.

Amsterdam Algoritmeregister. 2021. https://algoritmeregister.amsterdam.nl/en/ai-register/

Amsterdam-Amstelland safety region. 2020. "One and a Half Meter Monitor." Amsterdam: City of Amsterdam Algorithm Register. https://algoritmeregister.amsterdam.nl/en/one-and-a-half-meter-monitor/

Andraško, Jozef, Matúš Mesarčík and Ondrej Hamuľák. 2021. "The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework." AI & Soc (2021). doi: 10.1007/s00146-020-01125-5.

Article 29 Data Protection Working Party. 2007. "Opinion 4/2007 on the concept of personal data." https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Assemblée Nationale. 2018. "Rapport N°1335 : Rapport d'Information." https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information.pdf

Barelli, Paul. 2018. "A Nice, l'application sécuritaire Reporty divise les habitants." Le Monde, 6 February 2018. https://www.lemonde.fr/societe/article/2018/02/06/a-nice-l-applicationsecuritaire-reporty-divise-les-habitants 5252467 3224.html.

Bensalem, Nawal. 2018. "La police belge mise gros sur la reconnaissance faciale : découvrez les techniques scientifiques de demain." La Dernière Heure, 24 September 2018. https://www.dhnet.be/actu/faits/la-police-belge-mise-gros-sur-lareconnaissance-faciale-decouvrez-les-techniques-scientifiques-de-demain-5ba7ff06cd70a16d81022de6.

Binacchi, Fabien. 2019. "Vos émotions analysées pour des raisons de sécurité? Un test proposé à Nice." 20 Minutes, 15 January 2019. https://www.20minutes.fr/high-tech/2423167-20190115-nice-si-emotions-analysees-raisons-securite-ville-etudie-question-opposition-offusque

BPI France. 2018. "Le projet innovant SafeCity, pour renforcer la sécurisation des villes intelligentes sur le territoire, obtient un financement du Programme d'Investissements d'Avenir (PIA)." https://presse.bpifrance.fr/investissements-davenirle-projet-innovant-safecity-pour-renforcer-la-securisation-des-villes-intelligentes-sur-le-territoire-obtient-un-financement-du-programme-dinvestissements-davenir-pia/

Breyer, Patrick et. al. 2021. "MEP's Letter to the Commission on Artificial Intelligence and Biometric Surveillance". Brussels, 15 April. https://www.patrick-breyer.de/wp-content/uploads/2021/04/MEP-Letter-to-the-Commission-on-Artificial-Intelligence-and-Biometric-Surveillance.pdf (July 23, 2021).

Breyer, Patrick, and et. al. 2021. 'MEP's Letter to the Commission on Artificial Intelligence and Biometric Surveillance'. https://www.patrick-breyer.de/wp-content/uploads/2021/04/MEP-Letter-to-the-Commission-on-Artificial-Intelligence-and-Biometric-Surveillance.pdf (July 23, 2021).

Bröckling, Marie. 2019. "Gerichtsurteil zu Gesichtserkennung: Datenschützer scheitert an Löschung biometrischer G20-Datenbank." Netzpolitik.org, 24 Ocotber 2019. https://netzpolitik.org/2019/datenschuetzer-scheitert-an-loeschung-biometrischer-g20-datenbank/.

Bundeskriminalamt. n.d. "Gesichtserkennung." https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Kriminaltechnik/Biometrie/Gesichtserkennung/gesichtserkennung_node.html

Bundespolizei. 2019. "Test intelligenter Videoanalyse-Technik." https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2019/06/190607_videoanalyse.html.

Bundespolizeipräsidium Potsdam. 2018. "Teilprojekt 1. Abschlussbericht." https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf;jsessionid=B00C5E4B9341D9F8733EF8508A6D9C46.2_cid324?__blob=publicationFile&v=1.

REFERENCES

Buolamwini, Joy and Timnit Gebru. 2018. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." Proceedings of Machine Learning Research 81.

Caspar, Johannes. 2018. "Einsatz der Gesichtserkennungssoftware „Videmo 360" durch die Polizei Hamburgzur Aufklärung von Straftaten im Zusammenhang mit dem in Hamburg stattgefundenen G20-Gipfel." Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 18 December 2018. https://datenschutz-hamburg.de/assets/pdf/Anordnung_HmbBfDI_2018-12-18.pdf

Chaos Computer Club. 2018. "Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg." https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz

Chin, Josh and Clément Bürge. 2017. "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life." Wall Street Journal, 19 December 2017. https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355, checked on 4/24/2021.

CNIL. 2018. "Mise en œuvre expérimentale de l'application « REPORTY » par la ville de NICE : quelle est la position de la CNIL ?" https://www.cnil.fr/fr/mise-en-oeuvre-experimentale-de-lapplication-reporty-par-laville-de-nice-quelle-est-la-position-de.

CNIL. 2019a. "Délibération n° 2019-001du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail." https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf

CNIL. 2019b. "Reconnaissance faciale - pour un débat à la hauteur des enjeux." Paris: Commission National Informatique et Libertés.

Cochior, Cristina. and Ruben van de Ven. 2020. "Plotting Data: Acts of Collection and Omission." http://plottingd.at/a/introduction.html

Colomé, Jordi Pérez. 2019. "Marbella, the biggest video surveillance lab in Spain." EL PAÍS. 29 November 2019. https://english.elpais.com/elpais/2019/11/27/inenglish/1574849134_892168.html.

Council of Europe. 2018. "The Practical Guide on the Use of Personal Data in the Police Sector." https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

Council of Europe. 2020. "Digital Solutions to Fight Covid-19. 2020 Data Protection Report." https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c

Council of Europe. 2021. "Guidelines on Facial Recognition." https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

Csaky, Zselyke. 2020. "Nations in Tranzit 2020. Dropping the Democratic Facade." Freedom House. https://freedomhouse.org/sites/default/files/2020-04/05062020_FH_NIT2020_vfinal.pdf .

De Halleux, Françoise. 2020. 'Reconnaissance faciale: le ministre de l'Intérieur, Pieter De Crem, n'y renonce pas! (29/06/2020)'. Édition digitale de Liège. https://lameuse.sudinfo.be/591608/article/2020-06-29/reconnaissance-faciale-le-ministre-de-linterieur-pieter-de-crem-ny-renonce-pas (September 29, 2021).

De Hert, Paul. 2017. "Courts, privacy and data protection in Belgium: Fundamental rights that might as well be struck from the Constitution" in Brkan, Maja and Psychogiopoulou, Evangelia. Courts, Privacy and Data Protection in the Digital Environment, Maastricht: Edward Elgar, 63-81.

Défenseur des Droits. 2021. Technologies Biométriques : L'impératif Respect Des Droits Fondamentaux. Paris: Défenseur des Droits. https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/rap-biometr-num-08.07.21.pdf (September 29, 2021).

Delver, Guido. 2021. Phone interview on 29-03-2021. Interviewer: Ruben van de Ven

Dercsényi, Dávid. 2018. "Totális megfigyelés 50 milliárdért - Pintérék terve kiakasztotta az adatvédelmi biztost". hvg.hu. 2 December 2018. https://hvg.hu/itthon/20181202_NAIH_50_milliardos_totalis_megfigyeles_lenne_Pinterek_kamerarendszere.

DPA Hamburg. 2018. "Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg." Hamburg: DPA Hamburg. https://datenschutz-hamburg.de/assets/pdf/Pruefbericht_Gesichtserkennungssoftware.pdf

Dudebout, Camille. 2020. "Safe City Project in Nice: Testing Facial Recognition." https://ai-regulation.eu/safe-city-projectin-nice-testing-facial-recognition/.

EDPB 2019. Guidelines 3/2019 on processing of personal data through video devices, edpb.europa.eu. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.

EDPB. 2021a. "EDPB & EDPS Call for Ban on Use of AI for Automated Recognition of Human Features in Publicly Accessible Spaces, and Some Other Uses of AI That Can Lead to Unfair Discrimination | European Data Protection Board." https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en.

EDPB. 2021b. "Thirtieth Plenary Session: EDPB response to NGOs on Hungarian Decrees and statement on Article 23 GDPR." https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungari-

REFERENCES

an-decrees-and-statement-article_en.

EDPS and EDPB. 2021. "Joint Opinion on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)" https://edps.europa.eu/data-protection/our-work/publications/opinions/joint-opinion-edps-edps-proposal-regulation-european_en

EDPS. 2020. Shaping a Safer Digital Future: a New Strategy for a New Decade. Released 30 June 2020. https://edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en. Accessed on 16 March 2021.

EDPS. 2021. "Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary." https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en

EDRi. 2020. "Ban Biometric Mass Surveillance!" https://edri.org/our-work/blog-ban-biometric-mass-surveillance/

EDRi. 2021. "EU's AI law needs major changes to prevent discrimination and mass surveillance." https://edri.org/our-work/eus-ai-law-needs-major-changes-to-prevent-discrimination-and-mass-surveillance/

Eichenhofer, Johannes. and Cristoph. Gusy. 2017. "Court, privacy and data protection in Germany: Informational self-determination in the digital environment." In Courts, Privacy and Data Protection in the Digital Environment, eds. Masa Brkan and Evangelia. Psychogiopoulou,101-119. Edward Elgar.

Europan Commission. 2020a. Shaping Europe's Digital Future. Brussels: European Commission. https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

European Commission. 2018a. "Communication from the commission to the European Parliament, the European council, the council, the European economic and social committee and the committee of the regions Artificial Intelligence for Europe. {SWD(2018) 137 final}" https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.PDF.

European Commission. 2018b. "Coordinated plan on artificial intelligence (COM(2018) 795 final)." https:// ec.europa.eu/knowledge4policy/publication/coordinated-plan-artif icial-intelligence-com2018-795-final en.

European Commission. 2020b. White Paper on Artificial Intelligence: A European Approach to Excellence and Trust. Brussels: European Commission. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

European Commission. 2021a. Fostering a European Approach to Artificial Intelligence. COM(2021)205 (21 April) https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence.

European Commission. 2021b. Proposal for a Regulation of the European Parliament and the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM(2021) 206 Final. Brussels:

European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

European Economic and Social Committee. 2018a. "Trust, privacy and security for consumers and businesses in the Internet of Things (IoT)." https://www. eesc.europa.eu/en/our-work/opinions-information-reports/opini ons/trust-privacy-and-consumer-security-internet-things-iot-owninitiative-opinion.

European Economic and Social Committee. 2018b. "Artificial intelligence: anticipating its impact on work to ensure a fair transition." https://www. eesc.europa.eu/en/our-work/opinions-information-reports/opini ons/artif icial-intelligence-anticipating-its-impact-jobs-ensure-fairtransition-own-initiative-opinion.

European Economic and Social Committee. 2018c. "Artificial intelligence—the consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society." https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/ artificial-intelligence-consequences-artificial-intelligence-digit al-single-market-production-consumption-employment-and.

European Parliament. 2017. "European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics." https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051EN.html. Accessed 16 March 2020.

European Parliament. 2021. "European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice." https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html. Accessed 16 March 2021.

European People's Party. 2021. "Facial recognition software: regulation instead of ban." https://www.eppgroup.eu/newsroom/news/facial-recognition-software-regulation-instead-of-ban.

Europol. 2020. "Europol reply to written questions from MEP Chinnici and MEP Breyer to the Joint Parliamentary Scrutiny Group (JPSG)." https://web.archive.org/web/20201101141435/https://secure.ipex.eu/IPEXL-WEB/dossier/files/download/8a8629a87398b8340173b84ac84115eb.do

Farge, Rémy. 2020. "Police du futur et nouvelles technologies du profilage ethnique." La Chronique de la Ligue des Droits Humains (191): 13–16.

REFERENCES

Fernandez, Valérie, Jessica Galissaire, Léo Laugier, Guillaume Morat, Marine Pouyat, and Annabelle Richard. 2020. Facial Recognition: Embodying European Values. Paris: Renaissance Numérique. https://www.renaissancenumerique.org/ckeditor_assets/attachments/548/report_facial_recognition.pdf

FRA. 2018. Preventing Unlawful Profiling Today and in the Future: A Guide. Luxembourg: Publications Office of the European Union. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

FRA. 2019. Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement. https://op.europa.eu/publication/manifestation_identifier/PUB_TK0320019ENN

France 3 Auvergne-Rhône-Alpes. 2019. St Etienne : Des Capteurs Sonores à l'écoute de La Ville. https://www.youtube.com/watch?v=KyClOCiTqkU

Fussey, Pete and Daragh Murray. 2019. "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology". Colchester, UK: Human Rights Centre, University of Essex. http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf.

Galič, Maša and Raphaël Gellert. 2021. "Data Protection Law beyond Identifiability? Atmospheric Profiles, Nudging and the Stratumseind Living Lab". Computer Law & Security Review 40: 105486. https://doi.org/10.1016/j.clsr.2020.105486

Garstka, Krysztof. 2018. 'Between Security and Data Protection: Searching for a Model Big Data Surveillance Scheme within the European Union Data Protection Framework', HRBDT Occassional Paper Series https://www.hrbdt.ac.uk/download/between-security-and-data-protection-searching-for-a-model-big-data-surveillance-scheme-within-the-european-union-data-protection-framework/

Gehrke, Laurenz. 2020. "Hungary No Longer a Democracy: Report." Politico, 6 May. https://www.politico.eu/article/hungary-no-longer-a-democracy-report/.

Gonzalez Fuster, Gloria. 2020. Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights (PE 656.295). Brussels: European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf.

Gotink, Bart. 2019. "Slimme camera's herkennen elke carnavalsvierder in Korte Putstraat: 'Wie er niet in mag, hebben we er zo uitgepikt". bd.nl. March 6. 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/

Greenleaf, Graham. 2016. Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives. Rochester, NY: Social Science Research Network. SSRN Scholarly Paper. https://papers.ssrn.com/abstract=2892947 (July 25, 2021).

Gröhn, Anna. 2017. « G20-Überwachungstechnik filmt weiter: Großer Bruder Telemichel". Die Tageszeitung : Taz. https://taz.de/!5457108/.

Hamada, Wael. 2020. "Data-Lab." Inbraakvrije Wijk. https://inbraakvrijewijk.nl/big-data/

Hassani, Jamal E. 2019. "Expérimentation de reconnaissance faciale : Nice ravie, la Cnil sceptique."JDN, August 28. https://www.journaldunet.com/economie/services/1443319-reconnaissance-faciale-nice-ravie-la-cnil-sceptique/.

Henning, Maximilian. 2019. Überwachung am Südkreuz soll jetzt Situationen und Verhalten scannen. Netzpolitik.org. https://netzpolitik.org/2019/ueberwachung-am-suedkreuz-soll-jetzt-situationen-und-verhalten-scannen/

Herczeg, Márk. 2019. 'A Totális Megfigyelés Ellen Senki Sem Tüntet, Pedig Jó Úton Haladunk Felé'. 444. 24 April. https://444.hu/2019/04/24/a-totalis-megfigyeles-ellen-senki-sem-tuntet-pedig-jo-uton-haladunk-fele.

Het Parool. 2017. Camera's in billboards op Centraal Station voorlopig uit. Het Parool. https://www.parool.nl/gs-bd97c612

Hidvégi, Fanny and Zágoni, Rita. 2016. 'How Technology Enhances the Right to Privacy - A Case Study on the Right to Hide Project of the Hungarian Civil Liberties Union', Journal of National Security Law & Freedom, Vol. 8, 531.

Hillman, Jonathan and Maesea McCalpin,. 2019. "Watching Huawei's 'Safe Cities'". CSIS Briefs. Washington: Centre for Strategic and International Studies

Houwing, Lotte. 2020. "Stop the Creep of Biometric Surveillance Technology", European Data Protection Law Review, Vol. 2, 174.

Hungarian Parliament. 2019. Bill T/7690. 2019. T/7690. https://www.parlament.hu/irom41/07690/07690.pdf.

INCLO 2021. "In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World". Geneva & Buenos Aires : INCLO. https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf.

Intelligent Lighting Institute. n.d. "Stratumseind." Eindhoven University of Technology. https://www.tue.nl/en/research/research-institutes/top-research-groups/intelligent-lighting-institute/infrastructure/stratumseind/.

Interpol, 2020. Facial Recognition Fact Sheet. Lyon: Interpol. https://www.interpol.int/en/content/download/15013/file/FS-04_Facial%20R_Factsheets_EN_2020-03.pdf

REFERENCES

IPVM Team. 2020. Facial Recognition 101. Bethlehem PA (USA: IPVM

IPVM Team. 2021a. Video Analytics Fundamentals Guide. Bethlehem PA (USA: IPVM

IPVM Team. 2021b. Facial Recognition Guide. Bethlehem PA (USA: IPVM

Jasserand, Catherine. 2016. "Legal Nature of Biometric Data: From Generic Personal Data to Sensitive Data". European Data Protection Law Review (EDPL) 2: 297.

Jiaquan, Zhou. 2018. "Drones, facial recognition and a social credit system: 10 ways China watches its citizens" South China Morning Post. https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china, checked on 4/24/2021.

Kaszás, Fanni. 2020. "Coronavirus: New App to Track Nearby Positive Cases Available to Download." Hungary Today. 14.05.2020. https://hungarytoday.hu/coronavirus-hungary-app-virusradar/

Kerékgyártó, Istvan. 2018. "Ami most épül, ahhoz képest Sztálin és Hitler titkosrendőrsége vaktában lövöldözött'." 24.hu https://24.hu/poszt-itt/2018/12/09/kerekgyarto-ami-most-epul-ahhoz-kepest-sztalin-es-hitler-titkosrendorsege-vaktaban-lovoldozott/.

Kindt, Els, Eva Lievens, Eleni Kosta, Thomas Leys, Paul De Hert. 2008. "Constitutional Rights and New Technologies in Belgium" in Leenes, Ronald, Bert-Jaap Koops, Paul de Hert, and Susan W. Brenner, eds. 2008. Constitutional Rights and New Technologies: A Comparative Study. The Hague : Cambridge ; New York: T.M.C. Asser Press ; Distributed by Cambridge University Press ; 11-55.

Kindt, Els. 2013. Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. Dordrecht: Springer Netherlands.

Kokkeler, Ben; Steven van den Oord; Steven van der Minne; Ilona Danen; Jason van Erve; Joelle van der Laan. 2020a. "De rol van sensoring bij coproductie van sociale veiligheid in een wijk: Een conceptueel model op basis van literatuurstudie en een analytische aanpak om digitale coproductie van sociale veiligheid in de wijk te toetsen". Breda : Avans Hogeschool. https://www.hbo-kennisbank.nl/details/sharekit_av:oai:surfsharekit.nl:ae9b7c0f-9a34-419a-b409-5b1792d805b3?q=ben+kokkeler&has-link=yes&has-link=yes&re-1-k=avanshogeschool&p=2

Kokkeler, Ben; Steven van den Oord; Steven van der Minne; Ilona Danen; Jason van Erve; Joelle van der Laan. 2020b. "Het Fieldlab Inbraakvrije Wijk Rotterdam: Een empirische verkenning naar de impact van sensoring ter bevordering van sociale veiligheid in de wijk Lombardijen". Breda : Avans Hogeschool. https://hbo-kennisbank.nl/details/sharekit_av:oai:surfsharekit.nl:c4baf1cd-4df6-4779-a330-43184094de95

Közbeszerzési Hatóság. 2020. "Táj. az elj. eredményéről-Szitakötő. fejlesztése". Budapest : Közbeszerzési Hatóság. http://www.kozbeszerzes.hu/ertesito/2020/0/targy/portal_403/megtekint/portal_9112_2020/.

Krol, Folkert van der. 2019. "Rotterdam Lombardijen is walhalla voor inbrekers". AD.nl. https://www.ad.nl/rotterdam/rotterdam-lombardijen-is-walhalla-voor-inbrekers-aba6ac9b/

L'Avenir. 2019. "La police fédérale doit mettre un terme à son projet de reconnaissance faciale à Zaventem." L'Avenir, September 20. https://www.lavenir.net/cnt/dmf20190920_01382727/la-police-federale-doit-mettre-un-terme-a-son-projet-de-reconnaissance-faciale-a-zaventem.

La Quadrature du Net. 2020. "Our Legal Action against the Use of Facial Recognition by the French Police". La Quadrature du Net. https://www.laquadrature.net/en/2020/09/21/our-legal-action-against-the-use-of-facial-recognition-by-the-french-police/

La Quadrature du Net. et al. 2019. "Open Letter: Ban Security and Surveillance Facial Recognition" 19 December 2019. https://www.laquadrature.net/en/2019/12/19/joint-letter-from-80-organisations-ban-security-and-surveillance-facial-recognition/

Lavrysen, Luc, Jan Theunis, Jurgen Goossens, Pieter Cannoot and Viviane Meerschaert 2017. "Developments in Belgian Constitutional Law: The Year 2016 in Review". International Journal of Constitutional Law 15(3): 774–84. https://doi.org/10.1093/icon/mox060

Lippens, Jan, and Michel Vandersmissen. 2019. "Topman federale politie: 'We gaan camera's met gezichtsherkenning inzetten in Zaventem'." Knack, July 10. https://www.knack.be/nieuws/belgie/topman-federale-politie-we-gaan-camera-s-met-gezichtsherkenning-inzetten-in-zaventem/article-longread-1485633.html.

Lum, Kristian, and William Isaac. 2016. 'To Predict and Serve?' Significance 13(5): 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Lumi. 2020. La control room di Venezia e la rete di videosorveglianza urbana • Lumi, 2020. . Lumi. URL https://www.lumi4innovation.it/control-room-venezia-videosorveglianza-urbana/

Ma, Alexandra. 2018. "China is building a vast civilian surveillance network — here are 10 ways it could be feeding its creepy 'social credit system'". Business Insider Nederland. https://www.businessinsider.nl/how-china-is-watching-its-citizens-in-a-modern-surveillance-state-2018-4/

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

REFERENCES

Malevé, Nicolas. 2020. 'On the Data Set's Ruins'. AI & Society. 10.1007/s00146-020-01093-w

Ministerium für Inneres, Digitalisierung und Migration. 2020. Antwort Auf Eine Kleine Anfrage Im Landtag von Baden-Württemberg: Zwischenergebnisse Des Pilotprojekts Zur 'Intelligenten Videoüberwachung' in Mannheim. Stuttgart, Germany. https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/8000/16_8128_D.pdf.

Monroy, Matthias. 2018. "Kritik an G20-Gesichtserkennung: 'Neue Dimension staatlicher Ermittlungs- und Kontrolloptionen'". https://netzpolitik.org/2018/kritik-an-g20-gesichtserkennung-als-neue-dimension-staatlicher-ermittlungs-und-kontrolloptionen/.

Monroy, Matthias. 2020. "INPOL-Datei: Deutlich mehr Gesichtserkennung bei Bundespolizei und Kriminalämtern", Netzpolitik.org. https://netzpolitik.org/2020/deutlich-mehr-gesichtserkennung-bei-bundespolizei-und-kriminalaemtern/.

Mozur, Paul. 2018. "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras". New York Times, 7/8/ https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

NAIH 2018. "GDPR Communique to Hungarian Government." Accessed 7 April 2021. https://www.naih.hu/files/

NAIH-5578-3-2018-J-181001.PDF.

NAIH. 2019. "A Nemzeti Adatvédelmi és Információszabadság Hatóság Beszámolója a 2018. évi tevékenységéről B/4542". https://www.naih.hu/eves-beszamolok

Najibi, Alex. 2020. "Racial Discrimination in Face Recognition Technology". Science in the News, 10/24/2020. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

NEC. 2021. Bio-IDiom — NEC's Biometric Authentication Brand. NEC. https://www.nec.com/en/global/techrep/journal/g18/n02/180203.html (accessed 7.14.21).

Nesterova, Irena. 2020. "Mass Data Gathering and Surveillance: The Fight against Facial Recognition Technology in the Globalized World". SHS Web of Conferences 74: 03006.

Newsroom. 2020. "Shaping Europe's Digital Future: What You Need to Know". Modern Diplomacy. 22 February. https://moderndiplomacy.eu/2020/02/22/shaping-europes-digital-future-what-you-need-to-know/.

Nice Premium. 2017. "La Smart City au service de la Safe City." Nice Premium, July 7. https://www.nice-premium.com/actualite,42/local,5/nice-la-smartcity-au-service-de-la-safe-city,21769.html.

Nieuwsuur. 2020a. "Hoe Algoritmes de Stad Besturen." https://www.youtube.com/watch?v=gJDA4t6llgY

Nieuwsuur. 2020b. Nieuwsuur #307 9-11-2020. NOS-NTR. https://www.npostart.nl/nieuwsuur/09-11-2020/VPWON_1310969

Nishiyama, Hidefumi. 2018. 'Crowd Surveillance: The (in)Securitization of the Urban Body'. Security Dialogue 49(3): 200–216. https://doi.org/10.1177/0967010617741436

NIST. 2010. Special Database 32—Multiple Encounter Dataset (MEDS). NIST. https://www.nist.gov/itl/iad/image-group/special-database-32-multiple-encounter-dataset-meds

OpenCV. 2021. About. OpenCV. https://opencv.org/about/

Organe de Controle de l'Information Policière. 2019. "Rapport de Visite et de Surveillance - Synthèse version publique. DIO19005" Brussels: Organe de Contrôle de l'Information Policière.

Organe de Controle de l'Information Policière. 2021. "Supervisory Body for Police Information." Brussels: Organe de Contrôle de l'Information Policière https://www.controleorgaan.be/en/.

Overgaard, S., 2019. "A Soccer Team In Denmark Is Using Facial Recognition To Stop Unruly Fans". NPR.org. URL https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans

Parliamentary Assembly of the Council of Europe. 2017 Recommendation 2102 (2017) on Technological Convergence, Artificial Intelligence and Human Rights, adopted on 28 April 2017. Strasbourg: Coucil of Europe.

Prins, Aliou. 2021. "Collecte des empreintes digitales, reconnaissance faciale… Notre vie privée en danger ?" Moustique. https://www.moustique.be/28152/collecte-des-empreintes-digitales-reconnaissance-faciale-notre-vie-privee-en-danger.

Purtova, Nazedha. 2018. Between the GDPR and the Police Directive: Navigating through the maze of information sharing in public-private partnerships. International Data Privacy Law, Vol. 8, 52.

Quevillon, Joey. 2012. 'Video Motion Detection and Tracking for Surveillance Applications'. Thesis University of Victoria. https://dspace.library.uvic.ca/handle/1828/4145.

Redactie Inbraakvrije Wijk. 2019. "Sensoren in Het Carlo Collodihof." Inbraakvrije Wijk https://inbraakvrijewijk.nl/sensoren-op-het-carlo-collodihof/

Redactie LikeJeWijk. 2021. "Update Fieldlab Inbraakvrije Wijk." Wijkgids Lombardijen. https://www.likejewijk.nl/

REFERENCES

lombardijen/update-fieldlab-inbraakvrije-wijk/

Renaissance Numérique, 2019. Reconnaissance Faciale: Quel regard des français? Paris: Renaissance Numérique. https://www.renaissancenumerique.org/ckeditor_assets/attachments/449/rn-sondage_reconnaissancefaciale.pdf

Rollet, Charles. 2021. EU Parliament Removes Hikvision, Citing Human Rights Abuses. Bethlehem PA (USA): IPVM. https://ipvm.com/reports/hik-eu

Schemm, Martin. 2018. "Einführung Der Automatisierten Gesichtserkennung Beanstandet". Hambrug: Hamburgische Beauftragte für Datenschutz und Informationsfreiheit der Freien und Hansestadt, https://datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360videmo360.

Schlagwein, Felix. 2020. "'Hungary Is No Longer a Democracy' Says Hungarian Legal Scholar". Deutsche Welle. Accessed 19 July 2021b. https://www.dw.com/en/hungary-is-no-longer-a-democracy-says-hungarian-legal-scholar/a-53442394.

Schouten, Socrates, and Teuntje Bril. 2019. "Volg Jij Nog Waar Je Gevolgd Wordt?" Smart Society Case nr. 1. Amsterdam: Waag; Den Haag: Vereniging van Nederlandse Gemeenten. https://waag.org/sites/waag/files/2020-07/VNG-SSC-1-Beslissen-over-slimme-technologie.pdf

Segal, Zach. 2020. Gait Recognition Examined. IPVM. Bethlehem, PA (USA). https://ipvm.com/reports/gait-recognition-surveilance

Shung, Koo Ping. 2020. 'Accuracy, Precision, Recall or F1?' Medium. https://towardsdatascience.com/accuracy-precision-recall-or-f1-331fb37c5cb9

Snow, Jacob. 2018. 'Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots'. American Civil Liberties Union. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

Spirk, Jozsef. 2019. "A Parkolóautomatákból Is Pintér Kamerái Pásztázhatják Az Arcokat." 24.Hu, 7 January 2019. Accessed 21 April 2021. https://24.hu/belfold/2019/01/07/terfigyelo-kamerak-belugyminiszterium-pinter-sandor-szitakoto/.

Statista. 2021. "Straftaten in Deutschland bis 2020". Statista, https://de.statista.com/statistik/daten/studie/197/umfrage/straftaten-in-deutschland-seit-1997/.

Stojkovski, Bojan. 2019. 'Big Brother Comes to Belgrade'. Foreign Policy. https://foreignpolicy.com/2019/06/18/big-brother-comes-to-belgrade-huawei-china-facial-recognition-vucic/

Stolton, Samuel. 2020. "EU Data Watchdog "very Worried" by Hungary's GDPR Suspension". Euractiv. 18 May 2020. https://www.euractiv.com/section/data-protection/news/eu-data-watchdog-very-worried-by-hungarys-gdpr-suspension/.

Suresh, Harini. 2019. 'The Problem with "Biased Data"'. Medium. https://harinisuresh.medium.com/the-problem-with-biased-data-5700005e514c

Sustainder. 2021. "Anne." https://sustainder.com/en/products/sustainder-anne.

Szalai, Anna. 2019. "A NER-testvér szemmel tart: jön a totális megfigyelés?" Magyarnarancs.hu, 24 March 2019. Accessed 7 April 2021. https://magyarnarancs.hu/belpol/a-ner-testver-szemmel-tart-117270.

Tasz. 2021. 'Surveilled but not consulted: Citizens living under constant technological surveillance'. TASZ. https://hclu.hu/en/articles/surveilled-but-not-consulted

Technopolice. 2021. Toulouse. Technopolice. URL https://technopolice.fr/toulouse/

TELEFI Project. 2021. Summary Report of the project "Towards the European Level Exchange of Facial Images". https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf

Thales Group. 2020. "Electronic ID cards in Belgium: the keystone of eGovernment." https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/belgium.

The Hague Security Delta. 2021. "Stratumseind." https://www.thehaguesecuritydelta.com/innovation/living-labs/lab/3-stratumseind.

UNHRC. 2019. 41st Session, UN Doc. A/HRC/41/41 (17 May 2019).

Untersinger, Martin. 2019. "La CNIL plaide pour un « code de la route » de la reconnaissance faciale."Le Monde, November 15.

Van Amelsvoort, Adri and, John Riemen. 2018. 'Meerluikfoto's van verdachten' Het Tijdscrhift voor de Politie. 6 November. https://www.websitevoordepolitie.nl/meerluikfotos-van-verdachten/

van Barneveld, D., D. Crover, and A. Yeh. 2018. Sensoren En de Rol van Gemeenten. VNG Realisatie Whitepaper Den Haag: VNG Realisatie. https://www.vngrealisatie.nl/sites/default/files/2019-03/Whitepaper%20Sensordata%E2%80%93pdf.pdf (March 24, 2021).

REFERENCES

van Brakel, Rosamunde. 2020. "ADM Systems in the COVID-19 Pandemic: Belgium." In Algorithm Watch, Automating Society Report 2020. https://algorithmwatch.org/en/automating-society-2020-COVID19/belgium.

van de Ven, Ruben. 2017. "Choose how you feel; you have seven options". Institute of Network Cultures. https://networkcultures.org/longform/2017/01/25/choose-how-you-feel-you-have-seven-options/

Vazquez, Coline. 2020. "Reconnaissance faciale : comment les forces de police y ont-elles recours en Europe?" L'Express, February 19. https://lexpansion.lexpress.fr/high-tech/reconnaissance-facialecomment-les-forces-de-police-y-ont-elles-recours-en-europe_2118639.html.

Venier, Silvia., and Mordini,Emilio. 2010. "Second-generation biometrics" in Finn, Rachel and David Wright PRESCIENT Deliverable 2: Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment https://prescient-project.eu/prescient/inhalte/download/PRESCIENT_D2.pdf

Verbeke, Hans. 2019. "De slimste camera's hangen in Kortrijk: Politie vindt 'de man met de blauwe trui' in mum van tijd" HLN. https://www.hln.be/kortrijk/de-slimste-cameras-hangen-in-kortrijk-politie-vindt-de-man-met-de-blauwe-trui-in-mum-van-tijd-af252dfc/

Verseck, Keno. 2020. 'Hungary and the EU: Viktor Orban's Battle with the Rule of Law". Deutsche Welle. https://www.dw.com/en/hungary-viktor-orban-rule-of-law-eu-budget/a-55581020.

Vincent, James. 2021. "Automatic gender recognition tech is dangerous, say campaigners: It's time to ban it." The Verge. (14 April) https://www.theverge.com/2021/4/14/22381370/automatic-gender-recognition-sexual-orientation-facial-ai-analysis-ban-campaign

ViNotion. 2020. "TV Program 'Nieuwsuur' about Luminaires with ViNotion Surveillance Software." http://vinotion.nl/en/press-releases/tv-program-nieuwsuur-about-luminaires-with-vinotion-surveillance-software/

Wagner, Ben. 2021. 'Whose Politics? Whose Rights? Transparency, Capture and Dual-Use Export Controls'. Security and Human Rights: 1–12. https://doi.org/10.1163/18750230-31010006

Wang, Maya. 2018. "Eradicating Ideological Viruses": China's Campaign of Repression Against Xinjiang's Muslims. New York: Human Rights Watch. https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.

Wazulin, Lisa. 2019a. "Klarer Vorteil für den Bürger". Mannheimer Morgen. https://www.mannheimer-morgen.de/orte/mannheim,_artikel,-mannheim-klarer-vorteil-fuer-den-buerger-_arid,1511931.html.

Wazulin, Lisa. 2019b. "Erschreckend gleichgültig – Kommentare". Mannheimer Morgen https://www.mannheimer-morgen.de/meinung/kommentare,_artikel,-kommentar-erschreckend-gleichgueltig-_arid,1512275.html.

Xie, Ning, Gabrielle Ras, Marcel van Gerven, and Derek Doran. 2020. 'Explainable Deep Learning: A Field Guide for the Uninitiated'. arXiv:2004.14545 [cs, stat]. http://arxiv.org/abs/2004.14545

ANNEX: CASES

CJEU Decisions

C-291/12 Michael Schwarz v Stadt Bochum ECLI:EU:C:2013:670.

Joined Cases C293/12 and C594/12 Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Others ECLI:EU:C:2014:238

C-582/14, Patrick Breyer v Bundesrepublik Deutschland ECLI:EU:C:2016:779

C-203/15 Tele2 Sverige AB v Post –och telestyrelsen and Secretary of State for the Home Department v Tom Watson and OthersECLI:EU:C:2016:970

Opinion 1/15 of the Court (Grand Chamber) ECLI:EU:C:2017:592

C-434/16 Peter Nowak v Data Protection Commissioner ECLI:EU:C:2017:994

Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others v Premier Ministre and OthersECLI:EU:C:2020:791.

ECtHR decisions

Klass and others v Germany (1979-80) 2 EHRR 214

Peck v UK (2003) 36 EHRR 41

PG and JH v UK (2008) 46 EHRR 51

S and Marper v UK (2009) 48 EHRR 50

Uzun v Germany (2011) 53 EHRR 24

Gaughran v The United Kingdom Appl No 45245/15 (13.06.2020)

Decisions of National Courts

French Constitutional Council, Decision N° 2004-492 DC of 2 March 2004

French Constitutional Council, Decision n° 2012-652 DC of 22 March 2012

Administrative Court of Marseille, Decision N°1901249 of 27 February 2020

Cour constitutionnelle, N° 2/2021, 14 January 2021

© Picture credits:
Matthew Henry (cover)
Unsplash

Study Commissioned on behalf of the Greens/EFA Campaign for a Ban of Biometric Mass Surveillance
https://www.greens-efa.eu/biometricsurveillance

60 rue Wiertz/Wiertzstraat 60
1047 Brussels, Belgium
www.greens-efa.eu
contactgreens@ep.europa.eu