EUROPEAN DIGITAL RIGHTS

Ban Biometric Mass Surveillance

A set of fundamental rights demands for the European Commission and EU Member States

On the use of technology for the untargeted mass processing of special categories of personal data in public spaces

European Digital Rights 12 Rue Belliard, 1040 Brussels www https://edri.org twitter @edri_org tel +32 (0) 2 274 25 70

Ban Biometric Mass Surveillance
A set of fundamental rights demands for the European Commission and EU Member States

Published on 13 May 2020 in Brussels

Lead author:
Ella Jakubowska, EDRi

Co-Lead author:
Diego Naranjo, EDRi Head of Policy

Layout by:
Rafael Hernández, EDRi Communications Intern

The EDRi Brussels office would like to express our enormous thanks the whole network for their time, advice, participation and support in producing this paper and to the 28 organisations that particpated in the consultation. In particular, the following organisations and individuals have been instrumental across multiple stages of researching, drafting, discussing and reviewing:

Access Now
ARTICLE 19
Lotte Houwing, Bits of Freedom
Digitale Gesellschaft Schweiz
Douwe Korff, Emeritus Professor of International Law
Drzavljan D
EFF
Homo Digitalis
La Quadrature du Net
Open Rights Group (ORG) and ORG Scotland
Privacy International (PI)

Table of Contents

1. Executive Summary 4
2. Introduction: Ban Biometric Mass Surveillance 7
3. Core Problem Definition 10
    3.1 Mass Surveillance 10
        3.1.1 Biometric Mass Surveillance in EU Law 12
    3.2 Power Imbalances, Biases, and lack of Accountability 13
    3.3 Function Creep and Normalisation 14
    3.4 (Re-) Identification and Tracking Over Time 15
    3.5 Social Control and Illegitimate Science 16
4. Rationale for EU Action 17
5. Policy Analysis & Discussion 19
    5.1 Fundamental Rights Law 19
        5.1.1 Biometrics and the Right to Dignity 22
    5.2 Data Protection Law 23
    5.3 Defining "Recognition": Considering Identification, Detection and Processing 26
    5.4 Comprehensive Analysis of Existing Biometric Systems 27
    5.5 Biometric Processing Outside the Scope of a Ban 28
6. Case Study Assessments 30
    6.1 Facial Recognition in Ampère High School, Marseille 30
    6.2. Other Case Studies with Assessment and Analysis 32
    6.3 Mass Surveillance for Public Health Purposes (COVID-19) 33
7. EDRi's Recommendations 35
    7.1 Recommendations: Ban Biometric Mass Surveillance 36
    7.2 European Commission White Paper on AI 38
    7.3 Preventing a Digital Dystopia 38

1. EXECUTIVE SUMMARY

Across the EU, highly intrusive and rights-violating facial recognition and other biometric processing technologies are quietly becoming ubiquitous in our public spaces. As the European Commission consults the public as part of its consultation on the *White Paper on Artificial Intelligence* (AI), EDRi - a network of 44 civil society organisations - calls on EU bodies including the European Commission, the European Parliament, plus all EU Member States, to ensure that such technologies are comprehensively and indefinitely banned in both law and practice. Given that the current regulatory and enforcement framework has not been successful in preventing Member States from deploying unlawful biometric mass surveillance systems, we urge the Commission to act now.

The use of biometric technologies for the untargeted mass processing of special categories of personal data, in particular biometric data in public places, creates serious risks of mass surveillance. This unjustifiably infringes on fundamental rights including privacy, data protection, equality, freedom of expression and information, freedom of assembly and association, due process and more. Such uses of biometric processing constitutes an objectification of people's intimate and personal qualities in a way that is so intrusive as to infringe on their human right to dignity. As this paper will demonstrate, **these deployments of untargeted mass biometric processing systems - whether by law enforcement, public authorities (such as schools or local councils), or private actors - do not meet the required justifications or thresholds of necessity or proportionality to be considered lawful for the level of violation and intrusion they create**. This threshold is demanded by the the Charter of Fundamental Rights, the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). The legal frameworks within which such activities take place often do not meet the requirements of "prescribed for by law" established under the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights, and fail to provide adequate, effective remedies against untargeted, unnecessary, disproportionate surveillance.

On the grounds elucidated in chapter 5 (*Policy Analysis and Discussion*) and for the reasons explained in chapter 3 (*Core Problem Definition*), EDRi calls on EU Member States,

as well as the European Commission as the guardian of the EU's fundamental rights treaties and in its competency with regard to European borders, to **permanently stop all biometric processing in public and publicly-accessible spaces, wherever it has the effect or potential effect to establish mass surveillance**. This call to action requires that:

1. *EU Member States* immediately **halt all biometric processing that could amount to mass surveillance in public spaces**, ensuring that both current and future deployments are included. This should be supported by **a political debate by the European Council** on the fundamental rights impacts of biometric mass processing in Member States;

2. *EU Member States*, under the auspices of the European Data Protection Board (EDPB) and national Data Protection Authorities (DPAs), **publicly disclose all existing and planned activities and deployments** that fall within this remit;

3. *EU Member States* **cease all planned legislation which establishes biometric processing** that could lead to mass surveillance in public spaces. Instead, clear and foreseeable laws should only allow for targeted identification checks that are proportionate to the issues and context, and provide for effective remedies against abuse. DPAs can play a role by **advising national regulators and requesting action** from their national governments;

4. *The European Commission*, in particular Directorate-General (DG) HOME and with reference to DG RTD for the Horizon2020 Programme, ensure that funding given to Member States for biometric research or deployment is for activities which are fully compliant with the Charter, including **immediately ceasing all funding for biometric processing programmes** which could contribute to mass surveillance in public spaces. All EU bodies who give operational support or advice to EU institutions, including but not limited to Europol, Frontex and the Fundamental Rights Agency (FRA), **ensure that Member States cannot use these technologies in a way which gives way to fundamental rights abuses**;

5. *The European Commission*, under the auspices of the EDPS's advisory role, **review and ex post facto evaluate on fundamental rights and data protection grounds all laws covering EU biometrics that contribute to or amount to mass surveillance** and, as appropriate, recast, repeal or provide appropriate guidance to Member States about safeguards;[1] and

1 Many ofthe relevant laws are analysed in the reportFundamental rights review of EU data collection instruments and programmes <http://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf>

6. *The European Commission* (in particular DGs GROW, CNECT and JUST as the Directorate-Generals leading the Commission's work on the White Paper on Artificial Intelligence (AI) and DG HOME in its capacity on borders) **implement, through legislative and non-legislative means** and if necessary, infringement proceedings and Court action, **an immediate and indefinite ban on biometric processing that leads to mass surveillance in public spaces.** This process must be done under the supervision and/or support of the European Data Protection Supervisor (EDPS), the European Data Protection Board (EDPB), the FRA and DPAs.

It is the role and responsibility of the European Union, in particular the European Commission, the Council of the EU and the European Parliament, with the support of the European Data Protection Board which also includes the European Data Protection Supervisor, the EU Fundamental Rights Agency (FRA), national Member States, the national Data Protection Authorities (DPAs) of every EU Member State and any other oversight bodies, to determine the appropriate methods to ensure that biometric mass surveillance is comprehensively stopped and banned in law, and in practice, across the EU.

In addition, this paper proposes further fundamental rights measures and safeguards, including the proper resourcing of national DPAs, the clearer interpretation of data protection law, and strict controls even for uses of biometric processing that do not contribute to establishing mass surveillance. We ask the EDPS and the EDPB to issue statements and guidelines calling for Member State action to halt and disclose mass biometric processing in public spaces, and encourage the European Council and European Parliament, in their legislative capacities, to provide political support and instigate debates. This could be well-complemented by Parliamentary resolutions and research reports.

We further encourage Members of the European Parliament (MEPs) – in particular the intergroup on Artificial Intelligence & Digital; the Committee of the Regions (CoR); the European Economic & Social Committee (EESC) and all stakeholders who care about protecting the EU's fundamental rights, freedoms and values to join this call to ban biometric mass surveillance.

2. INTRODUCTION: Ban Biometric Mass Surveillance

Nota Bene: *Work on this paper started before the COVID-19 pandemic. We believe that its findings and recommendations are as relevant, if not more so, in light of the situation, and demonstrate the need for action against all forms of bodily surveillance. See Section 6.3 on Mass Surveillance for public health.*

As of May 2020, at least 15 European countries have experimented with biometric technologies such as facial recognition in public spaces, for purposes which lead to mass surveillance.[2] They have deployed these systems in ways that often lack transparency and accountability, and in a concerning absence of proper necessity and proportionality assessments, adequate public warning, or societal debate.[3] These systems violate people's right to conduct their daily life in privacy and with due respect for their fundamental freedoms and dignity; have a chilling effect on their freedoms of expression and assembly; and put limits on their ability to participate in public, social or democratic activities. Given the centrality of appearance to personal identity and the general uniqueness and immutability of bodily characteristics, the use of biometric surveillance systems in public spaces can enable unlawful permanent intrusion into our autonomy, freedom and privacy on a mass scale across time and place.

Biometric processing is being used more and more, largely due to increased availability of public funding and advances in machine learning algorithms, which have made the mass-scale analysis of photographic, video and other material cheaper and more accessible. Despite these advances, the capture, processing and storage of biometric data

2 At a minimum, activities are happening in Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, the Netherlands, Poland, Romania, Serbia, Slovenia, Sweden, Switzerland and the UK.

3 The RSA, *Artificial Intelligence in the Police Force: A Force for Good?* (2020) <https://www.thersa.org/discover/publications-and-articles/reports/ai-police-force>

are problematic not just technically, but by their very nature, as over 80% of Europeans are against sharing their facial image with authorities.[4] Whilst procedural safeguards and rights to justice are at the core of the European Union's legal framework, the use of biometric technologies which can lead to mass surveillance inherently negates the basic procedures of police and criminal law by treating every person as a suspect in a perpetual, omnipotent line-up.

The heart of the problem lies in what facial recognition and other biometric processing mean for our societies, including how they can amplify existing inequalities and discrimination, and whether they fit with our conceptions of democracy, freedom, equality and social justice.

Data supervisory authorities including the French CNIL, the UK's ICO and Sweden's Datainspektionen have raised serious concerns that many current deployments are illegal.[5] Whilst EU data protection and fundamental rights legislation already regulates many aspects of biometric processing, this paper urges the EU to review whether existing laws and enforcement are sufficient in light of the size of the threat posed to our societies by biometric processing which may have the effect of mass surveillance. This paper demonstrates that at its core, biometric processing which has the potential to amount to mass surveillance is incompatible with the fundamental rights and freedoms, data protection law, democracy, and essential principles of the rule of law at the heart of the EU.[6] EDRi calls, therefore, on the European Commission and Member States to take a series of bold steps to permanently end the use of opaque, intrusive systems for the untargeted processing of biometric or associated special categories of personal data in public spaces.

4 Fundamental Rights Agency (2020) <https://twitter.com/EURightsAgency/status/1234804039449239553>

5 The CNIL (2019) <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>; EDPB (2019) <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en>; ICO (2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/live-facial-recognition-technology-police-forces-need-to-slow-down-and-justify-its-use/>

6 As the Fundamental rights review has stated, "[e]mphasis should now lie on the establishment of robust horizontal protections and safeguards for fundamental rights and corresponding data protection inspection and enforcement capabilities that can meet the requirements stemming from EU law and fundamental rights standards." <http://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf>

Key Definitions

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

Biometric processing – there are many types of biometric processing, which may be referred to invariably as recognition, identification, authentication, detection or other related terms, as well as (often opaque) ways of collecting and storing biometric data even if the data is not immediately processed, all of which are in scope of this paper. See section 5.3

Facial recognition – facial recognition is one type of biometric processing. The Article 29 Working Party defines facial recognition as the "automatic processing of digital images which contain the faces of individuals for identification, authentication/verification or categorisation of those individuals," whether or not individuals have consented or have knowledge of its use.[7]

Identification – distinguishing a person from a larger set of individuals. See sections 5.3 and 3.4.

Mass surveillance – any monitoring, tracking, and otherwise processing of personal data of individuals in an incriminate or general manner, or of groups, that is not performed in a "targeted" way against a specific individual. See section 3.1.

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

Public (including publicly-accessible) spaces – UNESCO defines a public space as "an area or place that is open and accessible to all peoples, regardless of gender, race, ethnicity, age or socio-economic level. [...] In the 21st century, some even consider the virtual spaces available through the internet as a new type of public space that develops interaction".[8] Our analysis includes public spaces like streets, parks, or hospitals, as well as privately-owned but publicly-accessible spaces such as shopping centers, stadiums, public transport and other public interest services. Our analysis also includes online spaces, as they have become an important part of civic debate, democracy and public participation.

Purpose(s) – this paper is concerned with uses of biometric processing where the purpose of a deployment will or could lead to establishing mass surveillance. See section 3.1 for more information.

7 Article 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN* (2012) 2; quoted in FRA *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (2019), 7 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>

8 UNESCO, *Inclusion Through Access to Public Space* (2017) <http://www.unesco.org/new/en/social-and-human-sciences/themes/urban-development/migrants-inclusion-in-cities/good-practices/inclusion-through-access-to-public-space/>

3. CORE PROBLEM DEFINITIONS

This chapter outlines the harmful societal, ethical and fundamental rights effects and outcomes generated by the deployment and use of untargeted biometric processing technologies in public spaces by any actor, whether public or private. These problems demonstrate the urgency of the EU Commission and Member States taking immediate action.

3.1 Mass Surveillance

The use of technology to process mass-scale biometric data, whether for law enforcement, public authority or commercial purposes, presents unique and grave threats to privacy and security.[9] The Council of Europe defines mass surveillance as any monitoring that is not performed in a "targeted" way against a specific individual, and the EU Fundamental Rights Agency (FRA) notes that an untargeted use "starts without prior suspicion".[10] In practice, mass surveillance measures will disproportionately impact already over-surveilled groups, for example migrants, poor communities and people of colour, which can increase systemic discrimination against them. Even when conducted in a targeted way, principles of privacy and due process require that authorities have particular lawful interest in, and reasonable suspicion of, an individual to justify surveilling them. Mass surveillance in public spaces, by contrast, relates to actions which impact on the public in general and which rely on watching them indiscriminately, without reasonable suspicion, sufficient possibilities for them to have knowledge of what is happening, ability to consent, nor the genuine and free choice to opt in or out.

Decades ago, and despite wide criticism,[11] CCTV cameras were implemented fervently yet untransparently all over the world, with the alleged goal of deterring crime. Even

9 Privacy International, *The police are increasingly using facial recognition cameras in public to spy on us*, (2019) <https://privacyinternational.org/long-read/2726/police-are-increasingly-using-facial-recognition-cameras-public-spy-us>

10 Council of Europe, *Factsheet on Mass Surveillance* (2018) 3 <https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e; https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_en.pdf>

11 Surveillance Studies Network, *A Report on the Surveillance Society* (2006) <https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf>

proponents of CCTV have found it difficult to prove that these cameras are effective in preventing crime, demonstrating only that they can be efficient in very limited, specific circumstances as part of investigation or prosecution.[12] Now these same systems can be updated with biometric analysis capacities for even greater levels of remote surveillance in order to watch not just what happens on a certain spot, but to follow who may be doing it.[13] The impacts upon freedom of expression and assembly are stark; mass surveillance means that people lose the right to be anonymous in public spaces.[14] As the German Constitutional Court put it in its famous 1983 *Census* judgment:

> *A person who wonders whether unusual behaviour is noted each time and thereafter always kept on record, used or disseminated, will try not to come to attention in this way. A person who assumes, for instance, that participation in a meeting or citizen initiative is officially recorded, and may create risks for him, may well decide not to exercise the relevant fundamental rights ([guaranteed in] Articles 8 and 9 of the Constitution). This would not only limit the possibilities for personal development of the individual, but also the common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens.*[15]

Because of the impact of mass surveillance on individuals, inferences based on such surveillance practices are fundamentally unreliable. For example, the CNIL notes that constant surveillance in public spaces can make seemingly normal attitudes and behaviours appear suspect, citing examples such as wearing sunglasses, having one's hood up and staring at the ground or at a phone.[16]

The ubiquity and intrusiveness of mass surveillance puts limits on everyone's participation in social, public and political life and, as noted in Census, impacts on their ability to live an autonomous life without having to adapt behaviours due to a fear of being constantly watched. It prevents people from exercising their political and civil rights.[17]

This places a heavy onus of proof on those seeking to justify its use.[18]

12 Michelle Cayford, *The effectiveness of surveillance technology: What intelligence officials are saying* (2017) <https://www.tandfonline.com/doi/full/10.1080/01972243.2017.1414721>

13 European Network Against Racism, *Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe* (2019) 6 <https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf>

14 ARTICLE 19, *The Right to Protest Principles: Background Paper* (2016) <https://www.article19.org/resources/the-right-to-protest-principles-on-the-protection-of-human-rights-in-protests/>

15 BVerfG, 15.12.1983, BVerfGE Bd. 65, S. 1 ff ("Volkszählungsurteil"), <https://www.bverfg.de/e/rs19831215_1bvr020983.html>

16 The CNIL, *Reconaissance Faciale: Pour un Debat La Hauteur des Enjeux* (2019) <https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux>

17 Amnesty International, *Russia: Intrusive facial recognition technology must not be used to crackdown on protests* (2020) <*https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/*>; OHCHR, *Human Rights Committee holds general discussion in preparation for a general comment on the right of peaceful assembly* (2019) <https://ohchr.org/en/newsevents/pages/displaynews.aspx?newsid=24378&landid=e>

18 Privacy International, *Protecting Civic Spaces* (2019) <https://privacyinternational.org/long-read/2852/protecting-civic-spaces>

3.1.1 Biometric mass surveillance in EU law

Mass surveillance is prohibited in EU law. The fundamental right to respect for private and family life and the protection of personal data are central to the Charter of Fundamental Rights of the European Union (herewith "the Charter"), the European Convention on Human Rights (ECHR) and other legally-binding instruments.[19] The Charter and ECHR also guarantee rights to dignity, freedom of expression, and freedom of assembly and association – all of which are seriously threatened by mass surveillance.[20] The General Data Protection Regulation (GDPR) sets out important principles for the protection of personal data, which results in a high legal barrier to mass data collection and processing. The Data Protection Law Enforcement Directive (LED) adds that special category data processing must be 'strictly necessary', which as Working Party 29 explains means that law enforcement agencies must "foresee precise and particularly solid justifications for the processing of such data",[21] and that it must be explicitly authorised under EU or Member State law.

Under the GDPR and the LED, some forms of personal data are especially sensitive and therefore enjoy enhanced protections. This includes the processing of biometric data such as faces or fingerprints when used for the purpose of uniquely identifying a natural person, and observations which could enable someone to identify or predict characteristics such as race, ethnicity, gender, sexual orientation, religion or health status. This means that proxies, such as may be used in public surveillance – like wearing religious accessories, or how we walk – are similarly protected, as are analyses of how we look, move or act which could expose sensitive information. European data protection law applies equally to information that we have made public, for example by posting photos or details of our activities on the internet.

Performing untargeted biometric recognition in public spaces, whether online or offline, relies on the indiscriminate collection, processing or storage of the above described sensitive personal data on a mass scale, without control and knowledge from the individuals being surveilled. It obscures the possibility of targeted use, as random passersby are an inherent feature of public spaces. This is different to targeted or personal uses such as unlocking one's personal phone, which are outside the scope of this paper, as such uses do not infringe on people's ability to enjoy public spaces. We re-iterate, however, that whilst the scope of this paper is focused on biometric processing which could or will lead to a sense of mass surveillance, we have serious concerns about the fundamental

19 Rights to privacy and data protection are enshrined in Arts. 7 and 8 of the Charter and 7 and 8 of the ECHR.

20 The Charter also establishes rights to dignity (Art. 1), freedom of expression (Art.11) and freedom of assembly and association (Art. 12). The corresponding sections in ECHR are the Preamble (by reference to the Universal Declaration of Human Rights) and Arts. 10 and 11 respectively.

21 European Commission, *Opinion on some key issues of the Law Enforcement Directive* (2017) 8 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178>

rights violations and potential abuses of power by authorities, private or even commercial entities when conducting any targeted or untargeted biometric processing in public spaces. Such surveillance must always be subject to strict controls and fundamental rights as outlined in Section 5.5.

Untargeted mass processing of biometric data in public spaces obscures the possibility of targeted use, as random passersby are an inherent feature of public spaces.

3.2 Power Imbalances, Biases and a Lack of Accountability

The use of biometric surveillance systems creates a dynamic where the powerful watch and the powerless are watched. It enables disproportionately powerful groups to further fortify their power over socially-marginalised groups such as people living in poverty or social exclusion, people of colour, or human rights activists. This raises important questions about ethics and social justice, in addition to fundamental rights concerns such as the structural inability to gain genuinely informed, free, and explicit consent for public biometric processing, making the watched even more subordinate.

Biometric processing is already being used to systematise the targeting of citizens expressing legitimate dissent (such as environmental activists) or marginalised groups such as migrants or people with insecure housing situations. Surveillance and profiling technologies are in essence sorting technologies: their purpose is to assess and codify risk, and to treat people differently as a result. In the context of highly-discriminatory categorisations of who is considered 'suspicious' or 'risky', and numerous examples of violence in cases of profiling, there is a great risk that over-policed communities will be more likely to suffer from mass surveillance by biometric technologies.[22] This is further exacerbated by the fact that input data, such as are used to train biometric recognition systems, are not neutral, but reflect and encode the biases and structural discrimination of the societies from which they are drawn. Within discriminatory structures, this bias and lack of accuracy can lead to traumatic repeated false identifications of people of colour and can exacerbate over-policing.

Facial data processing technologies have been shown to be biased against people of colour, in particular women of colour, having dramatically higher error (false positive or negative) rates for identifying them.[23] However, even if the technology is trained to accu-

22 European Network Against Racism, *Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe* (2019) <https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf>; Fundamental Rights Agency, *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (2019) 20 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>

23 Joy Buolamwini, Gender Shades (2018) <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>

rately identify all faces equally, this will not increase its respect for fundamental rights. Instead, it will become even more effective at profiling and targeting specific groups, when they have not even been suspected of committing a crime.[24] Moreover, profiling based on self-learning ("artificial intelligence") algorithms is effectively unchallengeable because even those operating the systems cannot explain the underlying reasoning. This is made worse by the well-known phenomenon of "computer bias": the tendency of individuals to uncritically accept a computer-generated prediction.[25] In a nutshell, if it is inaccurate, biometric mass surveillance is problematic; but if it is 100% accurate, it can be even worse.

The current deployment of biometric identification and surveillance systems in publicly-accessible spaces is occurring in a vacuum of state accountability or public oversight and in violation of constitutional privacy protections which are designed to defend people from abuses of state power.[26] Furthermore, private actors are gaining disproportionate power over the technology used by public authorities and law enforcement, with little or no accountability for their actions. From deliberately obfuscating the inner-workings of their technologies,[27] to profiting from exploitative policing practices (in the case of ClearviewAI)[28], the blurred involvement of private actors in developing biometric mass surveillance systems can give them power not only over people – but great influence over states, too.

3.3 Function Creep and Normalisation

Facial recognition and other biometric processing represents a massive increase in the capabilities for omnipresent surveillance, power imbalances between people and state (and private companies), and the potential for authoritarian abuse. There is already evidence that biometric systems which have been deployed for one use are re-deployed or abused in other, more sinister ways so that even if people have initially provided consent over the use of their biometric or genetic data for a specific purpose, they have little to no knowledge of, or power to correct or object to, the further processing of those data. Once infrastructure is in place, the existence of these systems creates new possibilities for expanded intrusion. Some of the initial reactions to the global coronavirus pandemic show that once this possibility exists, states may take advantage of technological in-

24 The Guardian, *Facial recognition technology threatens to end all individual privacy* (2019) <https://www.theguardian.com/commentisfree/2019/sep/20/facial-recognition-technology-privacy>

25 Douwe Korff and Marie Georges, *Passenger Name Records, data mining & data protection: the need for strong safeguards*, section I.iii, The dangers inherent in data mining and profiling (2015) <https://rm.coe.int/16806a601b>

26 For example, SHARE Foundation, Serbia: Unlawful facial recognition video surveillance in Belgrade (2019) <https://edri.org/serbia-unlawful-facial-recognition-video-surveillance-in-belgrade/>; Administrative Tribunal of Marseille found in 2020 that facial recognition in two schools violated fundamental rights <https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf>

27 Panoptykon Foundation, Black-Boxed Politics: Opacity is a Choice in AI Systems (2020) <https://en.panoptykon.org/articles/black-boxed-politics-opacity-choice-ai-systems>

28 EURACTIV, *After Clearview AI scandal, Commission 'in close contact' with EU data authorities* (2020) <https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/>

frastructures to watch people in ways that are well beyond the scope of managing the current situation.[29] Furthermore, the existence of surveillance infrastructure and its use in day-to-day life can lead to the false belief that being constantly watched, tracked and analysed is normal. To the contrary, democratic societies cannot and must not allow the normalisation of activities that bear the hallmark of authoritarian regimes. As UN Special Rapporteur David Kaye emphasises, surveillance technologies are dangerously uncontrolled, and both states and companies must step up to tackle this delta.[30]

3.4 (Re-)identification and Tracking Over Time

The risks to fundamental freedoms are further enhanced if data gathered through mass surveillance are analysed and used to create profiles that, in turn, are applied to individuals in a crowd or group in order to "identify" persons worthy of even more intrusive attention.[31] Regardless of the technology used or the method of personal data collection, biometric processing systems are designed to enable individual retrospective identification – a function which can increase over time as more and more data are linked through existing surveillance infrastructures, searchable databases, data from other public authorities, and biometric processing in public spaces. Even metadata and anonymised, pseudonymised or non-personal data can be used to infer sensitive, personal, identifiable information when combined with the vast sources at the disposal of public and private actors.[32] These ever-increasing surveillance networks create "permanent records" of our lives, interactions and behaviours without proper consent or genuine possibilities to opt out, and without the opportunity to return to lawful anonymity once we realise that this was the wrong way to go.

The increased capacity of states to track and identify individuals through facial recognition and other biometric processing is likely to disproportionately impact populations which are already highly policed, surveilled and targeted by abuse, including people of colour, Roma and Muslim communities, social activists, LGBTQ+ people and people with irregular migration status.[33] The combined impact of facial recognition technology and the pursued mass merging of European-wide biometric databases will pose even greater risks to safety, privacy and other fundamental rights for these communities.

29 The EU-wide example of bulk metadata collection shows how states collect information for a particular use (eg finding terrorists) but over time increase the scope to include non-violent crimes such as burglaries.

30 UN OHCHR, *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools* (2019) <https://ohchr.org/en/newsevents/pages/displaynews.aspx?newsid=24736>

31 See Douwe Korff and Marie Georges, footnote 25, pages 32 – 34 <https://rm.coe.int/16806a601b>

32 European Data Protection Board (EDPB), *Guidelines 3/2019 on processing of personal data through video devices* (2019) 16 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf>; see also Douwe Korff and Marie Georges, o.c. (footnote 25), 34 – 36.

33 PICUM, *Data Protection, Immigration Enforcement and Fundamental Rights* (2019) <https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf>

3.5 Social Control and Illegitimate Science

Once untargeted biometric processing in public spaces is normalised, and people can be identified and tracked across systems and locations, they can then be scored, categorised and assessed without ever knowing how or why this is happening or how it may affect their life.[34] With governments rushing to innovate with big data and become leaders in AI-enabled public services, the massive amount of data held by authorities and increasingly by commercial actors about our health, criminal records and many other personal details can be combined.[35] With the rise of mass surveillance, this can be linked to physical individuals on the streets and can log their interactions and movements in a way that creates a detailed, intimate pictures of people's lives.[36] This can be exploited for extreme uses such as social scoring and behavioural manipulation which become ultimately a question of control.

The use of biometric technology for evaluation of behaviour, motivations or character often lacks a scientific basis, for example so-called "affect recognition" or "behavioural prediction" which claim to be able to identify a person's emotions or intentions, but fundamentally threaten human dignity and autonomy. A recent meta-analysis of research on 'emotion science' by leading researchers in the field concluded that there is no scientific support for claims made by technology companies that they can 'detect' emotion through video analysis. The researchers stated that such initiatives rest on misunderstandings and that "the science of emotion is ill-equipped to support any of these initiatives."[37] Similar concerns apply to unproven attempts to use advanced statistical analysis to detect whether someone is lying in a video interview.[38] Such forms of dubious behavioral prediction remove the ability of individuals to consent to the processing of their biometric data, deprive them of their right to due process and to be properly informed, and removes the ability for them to seek explanation or redress when they suffer harm. Such violations of rights will fundamentally and irreversibly undermine people's trust in those that deploy biometric technologies.

34 World Privacy Forum, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* (2014) <www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf>

35 For an early survey of UK state databases, see Joseph Rowntree Reform Trust, *The Database State* (2009) <https://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf>. This showed that in sharing data "between health and social services, the police, schools, local government and the taxman", "fewer than 15% of the public databases assessed [were] effective, proportionate and necessary, with a proper legal basis".

36 The Guardian, *The New Normal* (2020) <https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay>

37 Barrett, Adolphs, Marsella, Martinez & Pollak, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements* (2019) 48 <https://doi.org/10.1177%2F1529100619832930>

38 The Intercept, *We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive* (2019) <https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/>. See also Anders Eriksson and Francisco Lacerda, *Charlatanry in forensic speech science: A problem to be taken seriously* (2007) <http://www.cs.columbia.edu/~julia/papers/eriksson&lacerda07.pdf>. More generally, see Douwe Korff, *The use of the Internet & related services, private life & data protection: trends & technologies, threats & implications*, Council of Europe (2007) 25 – 27.

4. RATIONALE FOR EU ACTION

The legal basis for deploying any biometric systems in public, whether in trial or full implementation, is unclear – and in some cases non-existent - in European and Member State national law. Many deployments have been carried out entirely without evidence of prior data protection impact assessments (DPIAs) and other safeguarding measures, despite the potential for many of these uses to contribute to unlawful mass surveillance and other fundamental rights abuses.[39] Three UN Special Rapporteurs have warned about biometrics systems. UN Special Rapporteur on Freedom of Association and Assembly, Clément Voule, expressed in his 2019 Report that "[t]he use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited."[40] The necessity and proportionality of such systems have been called into question by UN Special Rapporteur on the Right to Privacy, Joseph Cannataci.[41] Similar concerns have been raised about the impact on human rights defenders, journalists, politicians and UN investigators by UN Special Rapporteur on Freedom of Expression, David Kaye.[42]

Public or civic spaces are the physical and digital settings where people express themselves freely, formulate ideas, discuss them with like-minded people and groups, raise dissenting views, consider possible reforms, expose bias and corruption, and organise for political, economic, social, environmental, and cultural change.[43]

39 Under the GDPR Arts. 15, 35 and 36 and LED Arts. 27, 28 and 47, mass biometric processing clearly triggers the requirement under law to perform Data Protection Impact Assessments (DPIAs).

40 UN, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association* (2019) 15 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/141/02/PDF/G1914102.pdf?OpenElement>

41 Biometric Update, *UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition* (2018) <https://www.biometricupdate.com/201807/un-privacy-rapporteur-criticizes-accuracy-and-proportionality-of-wales-police-use-of-facial-recognition>

42 OHCHR, *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools* (2019) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736>

43 Privacy International, *Defending Democracy and Dissent* <https://privacyinternational.org/strategic-areas/defending-democracy-and-dissent>

The effect of mass surveillance technology may be that in the long-term, people self-censor their thoughts, words, and actions.

In February 2020, the European Commission released its "White Paper on Artificial Intelligence", laying out policy options for a wide range of Artificial Intelligence (AI) applications.[44] On facial recognition and other biometric processing, the paper proposed that – due to the fundamental risks posed by the use of the technology – it should automatically be considered "high risk", invoking mandatory conformity assessments. However, the paper did not go further to adequately consider the impact of these "high risk" applications on fundamental rights. Had it done so, we believe the logical conclusion would have been to ban biometric processing technologies for mass surveillance purposes.

These concerns are shared even by industry players: the President of Microsoft has warned that facial recognition risks creating Orwellian surveillance societies[45] and Amazon's shareholders rebelled against its biometric surveillance plans, citing threats to civil liberties[46].

Although biometric processing technologies typically involve the use of 'Artificial Intelligence' techniques (more specifically, machine learning), we believe that the precise technical implementation of these systems is far less important than their consequences: mass surveillance has the same impact on fundamental rights whether it is accomplished by a machine learning algorithm or a team of humans reviewing video footage, although AI may allow for mass surveillance on an unprecedented scale. The current legal accountability and vacuum in which biometric deployments are occurring, in conjunction with widespread concerns across businesses, civil society and the general public, means that there is a strong basis to demand that the EU takes action.

ACT NOW

44 European Commission COM(2020) 65, White Paper: On Artificial Intelligence – A European approach to excellence and trust (2020), <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>

45 Microsoft, *Facial Recognition: It's Time for Action* (2018) <https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/>

46 The New York Times, *Amazon's Facial Recognition* (2019) <https://www.nytimes.com/2019/05/20/technology/amazon-facial-recognition.html>

5. POLICY ANALYSIS & DISCUSSION

This chapter explores and analyses the legal and policy arguments for permanently stopping untargeted biometric processing in public spaces, using fundamental rights and data protection law to scrutinise the legitimacy, lawfulness, necessity and proportionality of untargeted biometric processing in public spaces. This analysis provides the justification for the set of actions, amounting to a ban on biometric mass surveillance, which are proposed in chapter 7.

Under the Charter, the ECHR, the GDPR and the LED, untargeted biometric processing in public spaces – even as a means to achieve legitimate public policy outcomes - cannot be considered necessary or proportionate because the size of the threat posed to sensitive personal data and the limitations that it places on our rights and freedoms means that it is never the least intrusive option. Its use creates conditions for unlawful mass surveillance and by its very purpose, constitutes a fundamental violation of human dignity. The CJEU Advocate General adds that "mass, indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference" with rights to privacy and data protection.[47] *Despite this, deployments of biometric technology which establish mass surveillance continue unchecked across the EU. Legislative fragmentation, enforcement challenges and a lack of resources (political, financial and human) for national Data Protection Authorities (DPAs) further compound the problem of the untransparent deployment of biometric technologies in violation of the GDPR, the LED and the Charter.*

5.1 Fundamental Rights Law

The Charter (Art. 52(1)) and the ECHR (Arts. 8-11) establish that any interference with fundamental rights – as must be anticipated by any deployment of biometric technologies - must be "provided for by law", "[s]ubject to the principle of proportionality" and applied only "if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." The

47 CJEU, C-362/14, Maximillian Schrems v Data Protection Commissioner, Advocate General's Opinion (2015) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-summary-0_en.pdf>

European Data Protection Supervisor (EDPS) provides stringent guidance about demonstrating necessity and proportionality.[48] By contrast, current deployments have largely failed to demonstrate these legal criteria.

The prohibition of mass surveillance can be found across European case law, and is often characterised by a lack of reasonable suspicion against the surveilled.[49] Notably, the case of *S. and Marper v UK* at the European Court of Human Rights (ECtHR) found the "blanket and indiscriminate" retention of biometric data to be a "disproportionate interference" with the right to privacy, as it failed to satisfy the requirements of the ECHR and could not be regarded to be "necessary in a democratic society".[50] Article 15 of the e-Commerce Directive (2000/31/EC) recognises that the general monitoring of internet users is intrusive and unlawful.

The ECtHR has held that measures such as covert surveillance for the purposes of detecting or preventing crime, or the sharing of CCTV footage as in the case of *Peck v UK*, fall within the ambit of Art. 8 of the Convention, which protects the right to private and family life, and has underlined that restrictions imposed upon this right should not unacceptably weaken the protection afforded by this right.[51] In the case of *Digital Rights Ireland*, for example, the Court of Justice of the European Union (CJEU) examined the compatibility of the Data Retention Directive 2006/24/EC with Arts. 7 and 8 of the Charter.[52] It took particular note of the fact that the Directive:

> cover[ed], in a generalised manner, all persons and all means of electronic communication [...] without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime" (para 57).

The Court noted that the measures were "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance" (para 37). This applies a fortiori to mass surveillance over all manners of behaviour by individuals who are not linked to suspected crime or threats to public order in public places. In Schrems I, the Court held that:[53]

48 EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (2019) <edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf. This draws on extensive case-law of the ECtHR and CJEU in which these principles were first developed. See *Sunday Times (I)* and *Handyside* judgments, ECtHR.

49 For case law, see *Digital Rights Ireland* (2014) CJEU and *Big Brother Watch and Others v the United Kingdom (*2018) ECtHR. For lack of reasonable suspicion, see *Zakharov v Russia* (2006) ECtHR.

50 ECtHR, *S. and Marper v the United Kingdom* (2008) para 125.

51 ECtHR, *S. and Marper v the United Kingdom* (2008) para 112; ECtHR; *Christine Goodwin v the United Kingdom* (2002); Peck v UK (2003) ECtHR. See also ECtHR Factsheet on mass surveillance <https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf>

52 Joined Cases C-293/12 and C-594-12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources & Others and Seitlinger and Others* (2014) ECR I-238.

53 Case C-362/14, *Schrems v Data Protection Commissioner* (2015) E.C.R. 627.

> legislation permitting public authorities to have access to the content of electronic communications on a generalized basis must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed in Art. 7 of the Charter ... (para 94)

Similarly, mass surveillance of the (offline or online) activities – including political, artistic or social activities – of large groups of people or even entire populations by means of indiscriminate collection and further use of biometric data undoubtedly also "adversely affects the essence" – the "untouchable core"[54] – of rights to privacy, freedom of expression and association. This occurs irrespective of any link between the great majority of those surveilled and any crime or threat to public order, and must therefore always be regarded as incompatible with the Charter. **In other words, a measure allowing for constant, real-time surveillance, especially involving the processing of sensitive, special-category data such as facial biometric data, in a blanket or indiscriminate manner, would per se violate the essence of fundamental rights such as privacy, dignity, freedom of expression and freedom of association and would thus be incompatible with EU law.**

Under the Charter, Titles V (Citizens' Rights) and VI (Justice) in particular establish a rigorous framework for due process, proper procedure, and the rule of law which ensure that citizens have access to information about how their affairs are being handled (Articles 41 and 42), access to an effective remedy and fair trials (Article 47) and the presumption of innocence (Article 48). This is complemented by Article 20 on the right to equality before the law.[55] These criteria bring important safeguards to ensure people are treated within a framework of democracy and justice; that states cannot arbitrarily abuse their power; and that people have knowledge over how they are being treated. The covert, remote and indiscriminate use of facial recognition and other biometric processing in public spaces, however, is a fundamental violation of these criteria as applied by the CJEU and the ECtHR.

> **It treats everyone as a potential suspect in a perpetual line up, which is at odds with freedoms and rights to live one's life with dignity, privacy, liberty, security, and the presumption of innocence.**

54 The concept of an "untouchable core" to all fundamental rights that may never be impinged upon, for any reason no matter how pressing or serious, was first developed in German constitutional law but is now recognised in international human rights law, and expressly stipulated in Art. 52 of the Charter. See: Pierre Thielbörger, *The "Essence" of International Human Rights*, German Law Journal (2019), 20, 924–939, <https://www.researchgate.net/publication/335615595_The_Essence_of_International_Human_Rights>

55 *Schrems v Data Protection Commissioner*, 2015 E.C.R. 627. In *Digital Rights Ireland*, the Court held that the "essence" of the right to privacy was not affected because, while the Data Retention Directive required the retention of communication metadata, it did not extend to the contents of the communications (para 39).

The fundamental rights-led approach in this paper demonstrates that mass surveillance is never permissible in the EU under the Charter, and so by definition the use of biometric processing in public spaces that leads to mass surveillance is already unlawful. Biometric processing is so intrinsically intrusive, and its functioning so conducive to of mass surveillance, that it must be specifically and indefinitely banned. In order to permanently stop this practice, responses by the EU must cover any actions or programmes that have the intention or effect of constituting or leading to mass surveillance, rather than specific technologies, which are liable to adaptation but will remain harmful as long as they can be used for mass surveillance and, therefore, control. Mass surveillance by its very nature is a fundamental breach of fundamental rights: it impinges on the very essence of privacy, data protection and other rights. Any use of biometric processing which interferes with the right to privacy without proper justification and thereby contributes to mass surveillance – even unintended – is within scope, regardless of whether the use is by law enforcement, public authorities, or commercial actors. The UK ICO notes that even for public policy purposes, most biometric technologies are developed and deployed through a combination of public and private actors.[56]

5.1.1 Biometrics and the right to dignity

Building on the fundamental rights implications described in Section 5.1, all EU fundamental rights are founded on the fundamental dignity of the person under Article 1 of the Charter, which states that "Human dignity is inviolable. It must be respected and protected." Other national and international human rights instruments are similarly centrally founded on universal and inalienable human dignity.[57] [Thi]This has led to dignity being considered a "motherright."[58] The use of mass surveillance in public for recognising, identifying or detecting special categories of personal data, however, is fundamentally in violation of the right to dignity, as it uses people's own qualities, behaviours, emotions or characteristics against them in ways that are not justified or proportionate in EU or national law. This leads to the unlawful and dignity-violating effects explored extensively in chapter 2. As FRA describes, the use of facial recognition can violate dignity by making people avoid important places or events; through excessively forceful/coercive ways that data might be collected; and through "inappropriate police behaviour", confirming that:[59]

> *"[T]he impact on what people may perceive as surveillance technologies on their lives may be so significant as to affect their capacity to live a dignified life."*

56 Information Commissioner's Office, Statement on Live Facial Recognition Technology in King's Cross (2019) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/>

57 Cf. the German constitutional (proto-)right of "[respect for the] human personality" (das allgemeine Persönlichkeitsrecht), and the principle at the basis of the French data protection law of 1978 (retained in all subsequent laws and now granted constitutional status) that "Informatics must serve mankind."

58 Barak, A.*Human Dignity: The Constitutional Value and the Constitutional Right* (2015) 156-169.

59 FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement (2019) 20 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>

The European Data Protection Supervisor (EDPS) expands on this, explaining that the commodification and objectification of people's faces, in particular by algorithms and for the benefit of private companies or state surveillance to be used against us at a mass scale - all of which are inherent elements of facial recognition - are in and of themselves an infringement of dignity.[60] Coupled with the intimacy and intrusiveness of tracking people's bodily characteristics, untargeted biometric processing in public spaces becomes an inherently dignity-violating practice. Its potential to be used for mass surveillance only serves to add to its incompatibility with fundamental rights. Lastly, as the right to dignity is inviolable, even when EU Member States take measures based on national security or to counter a public emergency, they must still always refrain from violations of dignity. Dignity thus forms a fundamental underpinning for the call for a ban on biometric mass surveillance.

5.2 Data Protection Law

The GDPR sets out rules for the processing of personal data, and applies to the processing of all personal data other than for law enforcement purposes (which is covered by the LED). Under Article 9(1), the processing of biometric data, as well as data that reveals other protected characteristics, is in principle prohibited due to the sensitivity of such data. Legitimate exceptions are made possible – for example on the basis of consent (Article 7) – although the deployment of mass monitoring in public spaces, which are an essential part of public life, fundamentally precludes the ability for people to give genuine, informed, freely-given consent, thereby violating their rights to data protection. As the example of Ampère School, Marseille, will demonstrate (Section 6.1), current deployments of biometric processing in public spaces have not adhered to the lawful basis requirement in Article 5 of the GDPR, and other examples have fundamentally contravenedthe GDPR's Art. 5 requirements including for data minimisation, meaning that data collected should be limited to what is necessary for clearly-defined and expressly specified legitimate purposes; purpose limitation; data quality requirements prohibiting the use of personal information that is insufficiently accurate; transparency, and the burden on the data controller to prove that they meet these requirements. Article 22 of the GDPR furthermore prohibits fully-automated decisions based upon, among other types, biometric data.

The LED sets out the rules for the processing of personal data by "competent authorities", most frequently (but not exclusively) law enforcement authorities in criminal procedures, when undertaken strictly for law enforcement purposes (such as the preven-

60 Wojciech Wiewiórowski, Facial recognition: A solution in search of a problem? (2019) <https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en>

tion, detection or prosecution of criminal offences). It was adopted at the same time as the GDPR as part of a combined package and is its sister instrument, based on the same principles. It too emphasises that '[t]he protection of natural persons in relation to the processing of personal data is a fundamental right".[61]

The LED reiterates that even for law enforcement purposes, data must be processed "lawfully and fairly" (Art 4(1)(a)). The LED additionally sets out distinctions between the treatment of criminal convicts or suspects (in which case law enforcement must have "serious grounds for believing that they have committed or are about to commit a criminal offence") (Article 6(a)) compared to those who are not convicted or suspected of criminal activity. **This distinction is important, because it demonstrates a difference between the legitimate and lawful targeting of a genuine suspect (subject to the suspicions meeting the LED's threshold for "serious grounds") and the illegitimate, indiscriminate targeting of the general public inherent to untargeted biometric processing.**

As in the GDPR, the processing of data for law enforcement purposes must meet strict criteria. Under the LED, such processing must be necessary (Article 8(1)), will have special requirements for sensitive – including biometric - data (Article 10), and must adhere to a long list of requirements for safeguards, due process/good administration, the right to information and "data protection by design and default" (Article 20(1)). Unlike in the GDPR, consent is not a legal basis. Working Party 29 adds that data processing for law enforcement must meet the high criteria of "*strict* necessity."[62]

Whilst some uses of biometric processing are clearly within the remit of the GDPR (for example queue management in shops, local authority activities such as in schooling) and others within the LED (judiciary, police law and order activities), the overlapping subject matter of the laws makes some scenarios ambiguous. For example, the following scenarios are unclear: a police database containing details of criminals, victims and witnesses; or police using a watchlist at a football game to identify known criminals – but in doing so, capture members of the crowd, which under the GDPR requires consent. For these reasons, some Member States have introduced combined national laws. For the purpose of this paper, the essential issues of biometric processing leading to unlawful mass surveillance, unjustified infringement of data protection rules, and a violation of dignity remain unchanged whether the GDPR or LED applies to the case of a specific deployment of the technology. Regardless, such legal grey areas demonstrate the urgent need for more interpretation of the laws by courts and data protection bodies and authorities.

61 Cf. the German constitutional (proto-)right of "[respect for the] human personality" (dass allgemeine Persönlichkeitsrecht), and the principle at the basis of the French data protection law of 1978 (retained in all subsequent laws and now granted constitutional status) that "Informatics must serve mankind."

62 European Commission, Opinion on some key issues of the Law Enforcement Directive (2017) 7-8 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178>

Such issues are further complicated by the growing role of private actors in law enforcement data processing, for example as a result of outsourcing or the provision of complicated technologies over which law enforcement officers may not have sufficient technical expertise. It is questionable whether such actors are in a position to comply with the LED or even the strict "explicit consent requirements" contained also in the GDPR, as well as strict confidentiality, security, safeguarding and prevention of abuse requirements.

Activities undertaken on national security grounds – which are the competence of national intelligence bodies, not law enforcement agencies – are not covered within the data protection rules under the LED.[63] Yet FRA highlights that even when it comes to national security issues "the mere fact that a decision concerns state security does not render EU law inapplicable [...] The 'national security' exception thus cannot be seen as entirely excluding the applicability of EU law."[64] Any processing undertaken on the basis of law enforcement (i.e. criminal matters) remains distinct from national security exemptions – which, FRA emphasises, are still subject to fundamental rights. By contrast, "public security" measures for law enforcement are considered within scope under Article 1(1)) of the LED. FRA clarifies this point, emphasising that "[a]n objective of general interest - such as crime prevention or public security – is not, in itself, sufficient to justify an interference" with fundamental rights, meaning the LED's data protections must apply.[65]

There is both an urgent requirement, and a great opportunity, for better enforcement and clearer interpretation (including through litigation) of the GDPR and the LED, and of the interrelations between them, such as in relation to the transfer of data from private entities to law enforcement agencies (and the further transfer or making accessible of such data to national security agencies),[66] in regards to protecting biometric and related sensitive data or closing loopholes that have been exploited. The adoption of the GDPR was welcomed by European civil society, but its implementation has not been consistent across the EU, giving Member States discretion over how to deal with certain violations.

63 Actions relating to "public security" and "law enforcement" (subject to EU law) versus "national security" (outside EU law) are increasingly interlinked. See Douwe Korff and Marie Georges, The DPO handbook (2019) section 1.4.3 <http://www.fondazionebasso.it/2015/wp-content/uploads/2019/07/T4DATA-MANUAL-2019.pdf > in particular "Scope of the LEDPD" (pp. 59 – 63) and section 1.4.6, 89ff, Transmission of personal data between different EU data protection regimes (which clarifies that transfers of personal data from entities subject to the GDPR to national security agencies of the Member States are subject to the GDPR, even if the actions of the receiving agencies are not subject to EU law, including the Charter). On rule of law requirements relating to national security activities generally, see the CoE Commissioner for Human Rights, Issue Paper on The Rule of Law on the Internet and in the wider digital environment (2014) section 4.6, 107 – 110 <https://rm.coe.int/ref/CommDH/IssuePaper(2014)1>

64 Fundamental Rights Agency, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume I: Member States' legal frameworks (2015) <https://fra.europa.eu/en/publication/2015/surveillance-intelligence-services-volume-i-member-states-legal-frameworks?_cldee=ZG5AZGllZ29uYXJhbmpvLmV1&urlid=1>

65 Fundamental Rights Agency, Facial recognition technology: fundamental rights considerations in the context of law enforcement (2019) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>

66 See Douwe Korff and Marie Georges, o.c. (footnote 62), section 1.4.6.

National data protection authorities (DPAs) have been inadequately resourced and politically disempowered by their Member States, meaning that their efforts to enforce the GDPR and LED have suffered, and actors in violation of the law have faced few incentives to comply. Ensuring that DPAs and other oversight bodies have specific privacy and biometric data expertise will further strengthen their ability to protect fundamental rights from biometric mass surveillance.

In sum, any biometric processing is seriously problematic because of the challenges that it poses to requirements for necessity, proportionality and the difficulty of demonstrating compliance with data protection law; as well as the inherent violation of dignity through the objectification of existential characteristics. However, once the possibility of untargeted (mass) processing in public spaces is added, such processing becomes near impossible to justify according to its stated purpose, and therefore becomes impermissible on data protection grounds.

5.3 Defining "Recognition": Identification, Detection and Processing

Under the GDPR, the processing of special categories of personal data including "for the purpose of uniquely identifying a natural person" is prohibited (except when explicitly allowed for under certain circumstances) (Art. 9(1)). Under Art. 10 of the LED, this is additionally only allowed when "strictly necessary". The terms "facial recognition" and "biometric recognition" are popular - but often imprecise - ways to describe a wide range of special category data processing activities.

The European Data Protection Board (EDPB) have confirmed that "identification" does not need to reveal someone's official name or identity, but includes any processing that makes it possible to distinguish one person from others,[67] which can be equally intrusive. This means that not only identification but also detection of appearance, inferred behaviour, predicted emotions or other personal characteristics are all within the scope of biometric processing as defined in the GDPR and if used in purposes that lead to mass surveillance, are within the scope of this paper.

The transient local analysis of user data (as opposed to transferring data to a central server) will not exempt uses of biometric recognition from being considered "processing". Nor will refraining from tracking users as they move from one camera to another exempt applications from being considered "identification". Both of these examples would remain within the relevant data processing obligations under the GDPR or LED. For these reasons, this analysis has not distinguished between recognition, identification or detection and has considered them all within the broader remit of processing.

67 EDPB, *Guidelines 3/2019 on processing of personal data through video devices* (2019) 16 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf>

5.4 Comprehensive analysis of existing biometric systems

FRA have expressed that, with the exception of a small number of the Member States researched, "[o]nly limited information is currently available on the possible use or tests of live facial recognition technologies in other EU Member States".[68] Considering the EU's responsibility to uphold fundamental rights, and the lack of evidence that deployments of biometric processing for mass surveillance are necessary, proportionate, or compliant with legal safeguards (such as Data Protection Impact Assessments), there is a clear need for greater public transparency of and accountability on the actors - whether public, private or a collaboration between the two - who are deploying biometric processing in public, as well as data exchanges between law enforcement, border security, other public security agencies (including health) and national security agencies. The example of Police Scotland demonstrates that it is both possible and advisable for law enforcement bodies to proactively respond to, and take steps to avoid, the fundamental rights issues raised by facial recognition.[69]

FRA, national data protection authorities (DPAs), civil society and the general public will all benefit from greater knowledge of biometric surveillance measures that are being taken in public spaces, in order to challenge the uses that violate fundamental rights. The burden must remain on the actors developing and deploying the technology to provide information about what they are doing to ensure that it complies with rights to information, procedural rights and all other fundamental rights and freedoms, too. The European Commission must ensure that a comprehensive study on the deployments, trials, and future planned deployments, motivations, legal bases, fundamental rights implications, involved actors and legal safeguards is undertaken for all biometric processing. Since the existence of what Statewatch has called the "EU security-industrial complex"[70] may lead (as suggested in the case of PNR systems[71]) to the promotion, defense and (ab) use of "securitisation" technologies, from CCTV cameras to "lie detectors" for refugees, we need to understand as a society who it is that develops these technologies and who benefits from doing so, at the expense of our rights and freedoms.

68 Fundamental Rights Agency, *Facial recognition technology:fundamental rights considerations in the context of law enforcement* (2019) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>

69 Following the release of Police Scotland's 2026 strategy, the Justice Sub-Comittee on Policing pressed the police in 2020 to confirm (a) they had no intention of rolling out facial recognition and (b) they agreed that they could not roll it out at this stage; Police Scotland agreed. See <https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology/JSPS0520R01.pdf> and <https://www.parliament.scot/S5_JusticeSubCommitteeOnPolicing/Inquiries/20200410_PstoJF_Facial_Recognitio....pdf>

70 Statewatch, *Market Forces: the development of the EU security-industrial complex* (2017) <http://www.statewatch.org/market-forces/index.htm>

71 EURACTIV, *The curious tale of the French prime minister, PNR and peculiar patterns* 2016, <https://www.euractiv.com/section/justice-home-affairs/opinion/checked-for-tuesthe-curious-tale-of-the-french-prime-minister-pnr-and-peculiar-patterns/>

In addition, DPAs in each member state could review if law enforcement authorities are using technologies in accordance with existing laws – with a particular emphasis on measures taken for supposedly "public security" purposes, which should be reviewed in light of the requirement of strict necessity (Article 10) - and clarify the role of the LED. The inclusion in the LED of a provision similar to Article 9(2)(g) of the GDPR – or simply the reading of the LED in that way by Courts and/or DPAs – would ensure that "substantial public interest" exclusions are not exploited as a loophole to justify uses of biometric processing which are otherwise unlawful.

5.5 Biometric processing outside the scope of a ban

EU law demands high ex ante standards for biometric processing. The European Data Protection Supervisor (EDPS) emphasises that necessity and proportionality are "an essential dual requirement with which any proposed measure that involves processing of personal data must comply."[72] In the case of using biometric data which contributes to mass surveillance, our analysis has demonstrated that these criteria cannot be satisfied because this impinges on the "essence" of fundamental rights protected by the Charter, in violation of Article 52(1). Such use is therefore inherently unlawful and should be banned, regardless of any arguments for any specific deployment in practice. Whilst increased accuracy will not increase the safety of biometric surveillance technologies, current issues around a lack of accuracy are nevertheless significant problems for public authorities or law enforcement looking to justify the necessity of the applications. At this stage, the necessity of a public use cannot be justified in the context of pilot deployments proving to have extremely high error rates.[73]

For uses that do not have the potential to be used for mass surveillance, every single deployment will nevertheless have to be subject to stringent ex ante rules (such as DPIAs, which in the case of mass biometric processing are required under the GDPR and the LED – see footnote 30) and requirements for ex post safeguards, and the entire development lifecycle must be compliant with all EU laws. This means that many non-mass surveillance uses of biometric data, such as the use of such data for targeted surveillance, individual, consensual authentication, protection of public health, or commercial uses may still be unlawful. The following example details the level of due diligence that must be taken on a case-by-case basis for biometric processing. Any use that cannot meet every step will be illegal.

72 EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (2019) 3 <edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf>

73 The Guardian, UK police use of facial recognition technology a failure, says report (2018) <https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure>

Law enforcement processing: demonstrating a "case by case" approach

When used by public authorities, for example in law enforcement, biometric technology without the potential to contribute to mass surveillance will still have to go through four cumulative steps of safeguards. First and foremost, human rights law requires that measures that interfere with fundamental rights be limited to what is strictly necessary and proportionate to the aim sought under Art. 52 of the Charter; this test provides a way to assess if a technology may ever, under law, be used. Secondly, legislative frameworks governing the use of biometric processing must satisfy legality or "in accordance with the law" requirements.[74] This means that the rules governing the deployment of the biometric data must satisfy strict accessibility, foreseeability and quality of the law requirements.

As a result, any authorisation and deployment of biometric processing must be explicitly prescribed by law and limited to cases that are strictly and demonstrably necessary to achieve a legitimate aim. That law must be accessible to the public and sufficiently clear and precise to enable persons to foresee its application and the extent of the interference. Among others, the law needs to provide for clear rules governing the retention, access to, amounts[75] and destruction of personal data obtained during the deployment of biometric processing that do not belong to the target(s) under investigation.

Third, the use of biometric processing for law enforcement must also be accompanied by safeguards in order to prevent abuse of this intrusive power. This at the very minimum includes transparency on criteria for inclusion on a watchlist;[76] the existence of individualised reasonable suspicion of involvement in a serious crime or threat that would justify deploying this technology;[77] prior Data Protection Impact Assessments (DPIAs) (LED recital 58) as well as prior consultation with relevant supervisory authorities (recital 28);[78] for individuals to be adequately notified of the processing of their biometric data and be given the opportunity to exercise their rights, especially of rectification, access, erasure, and to challenge processing operations by complaining before courts and regulators; and independent judicial or administrative authorisation and oversight to ensure rights including to legal remedy. It is crucial that even individuals whose biometric data are captured but against whom a case is not pursued (for example because they were not held to be the target of the surveillance) are informed at least ex post facto and granted remedies in the event that the data capture was unjustified or processed/shared/retained unlawfully. Releasing reliable and timely statistics on the capture and success rate of biometric data will ensure public confidence that these powers are not abused.

Fourth, authorities will be under an obligation to ensure the security and integrity of the personal data processed. Fundamentally speaking, the use of biometric technologies pertains to the processing of extremely sensitive personal data, through equipment which may have vulnerabilities or lack proper security safeguards to prevent unauthorised third-party access. For example, the hacking of just a single CCTV camera can affect many people, including those who are unrelated to a government operation. These fundamental human rights and rule of law requirements demonstrate that even in the absence of untargeted biometric processing, the use of biometric technologies for recognition, identification or other processing is subject to exceptionally strict controls under existing EU law.

74 Privacy International, *Briefing to the UN Counter-Terrorism Executive Directorate on the responsible use and sharing of biometric data to tackle terrorism* (2019) 3-4 <https://privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on%20biometrics%20final.pdf>

75 Fundamental Rights Review of EU data collection instruments and programmes, 44 <http://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf>

76 See *Big Brother Watch v United Kingdom*, para 387.

77 See *Szabó v. Hungary*, para 260.

78 This mirrors the requirements of the GDPR of a prior DPIA and possible prior consultation with the DPA for all processing operations that pose a high risk to the rights and freedoms of individuals – or indeed, if stipulated by law, the DPA's prior authorisation (Articles 35 – 36 GDPR).

6. CASE STUDY ASSESSMENTS

This chapter applies the arguments substantiated throughout this paper to real examples of biometric processing in public spaces which have led to mass surveillance. This is not an exhaustive list; in general, if the processing is untargeted, and in a public or merely publicly-accessible space; and has the potential to contribute to a perception of mass surveillence and/or a violation of dignity, then it will be included within what this paper argues is already illegal under EU law and must be banned in practice. The differences between the case studies demonstrates why it is so necessary for any deployment to be considered individually and for those developing and deployeing such tools and systems to engage in pre-deployment DPIA processes with national DPAs.

CASE STUDIES

6.1 Facial recognition in Ampère high school, Marseille

In July 2019, the Provence-Alpes-Côte d'Azur (PACA) regional authority asked France's data protection authority, the CNIL, for permission to use a facial recognition system for managing entry at Ampère high school in Marseille. This "trial" was intended to be a year-long experiment and was also being carried out at another school in the region (the Lycée les Eucalyptus in Nice) and was said to be held on the basis of students' and parents' consent.[79] The intention of the system was to facilitate the job of the schools' security agents, helping them to spot identity theft and to prevent access of unauthorised persons to the school. This was designed to increase the security of students and staff and to speed up the time it took for students to enter the school premises.

EDRi's analysis:

- **Objective**: as indicated by the CNIL, we agree that the system aims to achieve a legitimate public authority objective of managing entry into a school, to ensure that the right people could enter and the wrong people could not.
- **Necessity and proportionality**: as the CNIL emphasised, a school facial recognition system is not necessary when there is the less intrusive alternative of using identity badges. Furthermore, this use of facial recognition is disproportionate as it brings in a large-scale, intrusive data surveillance program against minors simply for the objective of school entry.[80]

79 The CNIL, *Experimentation de la reconnaisance faciale dans deux lycees* (2019) <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>

80 EDPS, *quick-guide to necessity and proportionality* (2018) <edps.europa.eu/sites/edp/files/publication/20-01-28_edps_quick-guide_en.pdf>

- **Other legality requirements**: under the GDPR, there are legal requirements for consent and for the minimisation of data. As confirmed by the CNIL and the Marseille regional Court, the Ampère facial recognition trial significantly violated both of these criteria, gathering data when it was unjustified, and being fundamentally unable to obtain legitimate consent due to the power dynamics between the public authority and students. Across EU law, young people are given enhanced protections (cf. Article 8 GDPR re information society services). Under GDPR, biometric data is considered highly sensitive (Article 9(1)). The biometric data of minors therefore requires the highest level of protections, which Ampère did not meet.

- **Severity of the risk**: using facial recognition to control school entry not only processes and retains minors' data unnecessarily and unlawfully, but could interfere with their fundamental right to access education by creating a culture of mistrust and surveillance in their place of learning or by putting pressure to conform on those that want to opt out. This was seen already in a Polish school found to be breaking the law by introducing a biometric system for assigning school lunches to pupils. Students were allowed to opt out – but were de facto punished by being made to wait until their 600 peers had received their food first.[81]

- **Other factors**: Other concerning factors in the case include the fact that the region seemed to deploy the experiment before obtaining the opinion of the CNIL, setting a dangerous precedent for a lack of state accountability. The decision by the PACA region to pilot such an intrusive system furthermore could suggest that the PACA region's data protection processes (for example DPIAs) are not being undertaken with due care for fundamental rights.

What this means:

Whilst the objectives of the system may have been acceptable, this analysis demonstrates that facial recognition for entry management in schools is neither a legitimate, necessary nor proportionate way to achieve this aim. The use of this mass biometric identification system in a school – which is not only a public space, but an essential one which young people are obligated to attend - is firmly within the scope of EDRi's call for a ban. The scale of the violations of young people's rights to privacy and data protection are so significant that even safeguards and DPIAs will not be able to make this sort of use compliant with Europe's fundamental rights laws.

The scale at which school entry systems operate greatly increases the potential for other violations. If replicated across European schools, there is potential for millions of young people to have their data unnecessarily and unlawfully processed on a daily basis. This could contribute to the normalisation of highly intrusive facial recognition, making properly-informed public debates less achievable.

There is widespread concern about the use of these technologies, and this means that there is a high chance of successfully informing policy decisions about the use of facial and biometric recognition in public mass surveillance scenarios like the case of Ampère high school. With both the CNIL and the regional Court of Marseille declaring this trial illegal, there is both a state and a public appetite to see potential violations of the rights of young people quashed at the earliest opportunity.

81 Urzad Ochrony Danych Osobowych, *Fine for processing students' fingerprints imposed on a school* (2020) <https://uodo.gov.pl/en/553/1102>

6.2 Other Case Studies with Assessment and Analysis

(a) Facial recognition software used to scrape social media

The ClearviewAI scandal in January 2020 raised public awareness about the risks that people's images, uploaded for social media and networking purposes, are being covertly used by private actors in ways that may help them build for-profit technology, and that also have been sold to the police.[82] This raises questions about the role and influence of private actors in law enforcement, problems with public procurement, and the potentially enormous discriminatory outcomes from inaccuracy, as well as the related issues of the (in)security of ClearviewAI's databases. But it is not just ClearviewAI: Facebook have been analysing users' photos for years in the name of being able to tag users, and other Big Tech corporations have similarly trained algorithms on reams of people's photos, without those people knowing the extent of how their data is used. The use of machine learning algorithms in this context provides further cause for concern: people whose faces are used for training data will face additional risks because their inclusion in training makes the system more likely to flag them.

The example of the EU Horizon 2020-funded SPIRIT project reinforces the lack of fundamental rights compliance, transparency and accountability in a social media scraping use case. Five law enforcement-related stakeholders participate in this research project: the Hellenic Police (GR), West Midlands Police (UK), Police and Crime Commissioner for Thames Valley (UK), Serbian Ministry of Interior (RS), and Police Academy in Szcytno (PL). According to the sparse and untransparent website, the project aims to use tools such as face extraction and matching, to correlate information from social media data, which constitutes a form of mass surveillance, and to continuously initiate complex associative searches over all sources relevant to criminal investigation.[83] According to freedom of information requests, trials were planned for 2020 and 2021, with genuine end users.[84]

(b) iBorderCtrl

The Horizon 2020 programme also funded a set of research projects on the Hungarian, Greek, and Latvian borders called iBorderCtrl.[85] The included one project to use automated analysis of biometric data to predict evidence of deception among those looking to

82 The New York Times, *The Secretive Company That Might End Privacy as We Know It* (2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>
83 SPIRIT (2018) <https://www.spirit-tools.com/index.php>
84 Ask the EU, Ref. Ares(2020)1351062 – 04/03/2020, <https://www.asktheeu.org/en/request/7495/response/25180/attach/2/REA%20reply%20confirmatory%20signed.pdf?cookie_passthrough=1>
85 iBorderCtrl <https://www.iborderctrl.eu/>

enter the EU. Freedom of information requests revealed that during the pilots in Greece, no real travelers participated in the Greek pilots,[86] and the project came to an end in August 2019. Under this paper's analysis of mass surveillance, such a use would not meet the criteria of indiscriminately processing the data of passersby. However, we believe that it would meet other criteria to be considered mass surveillance as the use of this technology is not targeted against specific individuals of lawful interest. Furthermore, such deception prediction "lie detector" tests can be considered part of the state mass surveillance apparatus because they rely on technologies of watching, with an unequal power dynamic and a use that is generally targeted against marginalised individuals. Following public scrutiny, the iBorderCtrl project team acknowledged the potentially harmful ethical implications of this project and the need for both public debate and a fundamental rights analysis.

6.3 Mass surveillance for public health purposes (COVID-19)

Since late 2019, the world has watched as the outbreak of Coronavirus in Wuhan quickly turned into a global pandemic. Public health responses have put unprecedented limits on the daily lives of people across the world. A range of important rights, especially the right to life, are of course threatened by the disease – but responses across the world can also threaten fundamental liberties and freedoms.[87]

Whilst taking proportionate public health measures is a legitimate policy action, there is a significant risk that the pandemic can be abused by states and private companies to smuggle in unlawful, highly-intrusive mass surveillance measures. In China, for example, purportedly benign, voluntary tracking and tracing apps[88] were quickly revealed to be automatically controlling people's access to public spaces and even sending their personal data to the police.[89] There are increasing calls for and attempts at the introduction of similarly threatening contact tracing apps across Europe, similar to Poland's mandatory facial recognition-based app used to enforce quarantine, which sends the police to the home of anyone that fails to share a selfie on the app within 20 minutes of an alert.[90]

Within the limits of this paper, we cannot discuss all of the implications of the Coronavirus pandemic and associated surveillance, nor of its intersection with biometric mass surveillance. Suffice to note that the mass collection and sharing of data, regardless of

86 Ask the EU, D6.4 Evaluation report of final prototype pilot deployment and Best Practices - Analysis of pilot feedback on final prototype (2019) <https://www.asktheeu.org/en/request/7488/response/24777/attach/3/D6%204%20700626%20Eval%20report%20final%20prototype%20pilot%20deploy%20BestPractices%20redacted.pdf?cookie_passthrough=1>

87 Fundamental Rights Agency, Protect human rights and public health in fighting COVID-19 (2020) <https://fra.europa.eu/en/news/2020/protect-human-rights-and-public-health-fighting-covid-19>

88 BBC, *China launches coronavirus 'close contact detector' app* (2020) <https://www.bbc.co.uk/news/technology-51439401>

89 New York Times, *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags* (2020) <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>

90 Gov.pl, Aplikacja „Kwarantanna domowa" – ruszya proces jej udostapniania (2020) <https://www.gov.pl/web/cyfryzacja/aplikacja-kwarantanna-domowa--ruszyl-proces-jej-udostepniania>

the context, can pose high risks to fundamental rights. We must be equally alert to the threats to fundamental rights and the rule of law that are shared by the use of biometrics that lead to mass surveillance in public spaces as explored in this paper, and many proposed apps and other technological "solutions" for tackling Coronavirus. We firmly believe that there is no justification for invoking derogation clauses in human rights treaties, in particular Article 15 ECHR, in order to depart from these requirements. As noted in Section 5.1, even in times of derogation, states may not impinge on the untouchable *essential core* of those rights.

The legitimation and normalisation of privacy-invading surveillance infrastructures risks creating a false sense that being watched and analysed all the time is acceptable, and contributes to societies filled with suspicion, abuse and mistrust. As the EU's Committee for civil liberties (LIBE) states, mass surveillance does not make us safer.[91] It puts undue limits on our liberties and rights which can continue long after a public emergency like the COVID-19 pandemic has been eased. EDRi has opened a section on its website to report and analyse on these developments.[92] There, we will argue for maintenance of full respect by all European states for all fundamental rights and principles, in relation to mass surveillance for public health purposes as much as in relation to mass surveillance for law enforcement or public order purposes. Different checks and balances may be required – but the fundamental principles and essential limits of state authority remain the same.

91 European Parliament, *Use of smartphone data to manage COVID-19 must respect EU data protection rules* (2020) <https://www.europarl.europa.eu/news/en/press-room/20200406IPR76604/use-of-smartphone-data-to-manage-covid-19-must-respect-eu-data-protection-rules>

92 EDRi, COVID-19 & Digital Rights Doc Pool <https://edri.org/covid-19-digital-rights-document-pool>

7. EDRi's RECOMMENDATIONS

The use of technology for the untargeted processing of biometric data (or proxy special categories of personal data) in public spaces, whether by law enforcement agencies, public authorities, or private/commercial actors, raises significant problems for fundamental rights and individual freedoms and must be taken seriously. The fundamental rights analysis conducted in this paper demonstrates that **biometric processing in public spaces that leads to, or has the potential to lead to, mass surveillance is incompatible with the EU fundamental rights framework, especially data protection, dignity, and the principles of necessity and proportionality, and is therefore illegal**. This remains true regardless of the stated purpose; and whether such mass surveillance effect is intentional or unintentional. **This is because mass surveillance represents an unjustified restriction on privacy and is even more intrusive when using biometric data, making its use inherently disproportionate**.

Four European instruments already prohibit biometric mass surveillance: in the broadest sense, the European Convention on Human Rights and the EU Charter of Fundamental Rights, and more specifically, the (Modernised) Council of Europe Data Protection Convention, the GDPR and its sister instrument, the LED. Data protection laws provide further barriers to biometric processing.

In practice, however, these instruments are not properly harmonised or uniformly applied, nor are they enforced fully. This has had the result that there have been many deployments of untargeted biometric processing amounting to mass surveillance in European public spaces that are incompatible with fundamental European law and principles. These deployments have violated fundamental rights including rights to dignity; liberty; security; privacy; data protection, especially data minimisation, data protection by design and default, and consent; equality and non-discrimination; freedom of expression; freedom of assembly and association; freedom of information; and justice, including the right to an effective remedy and to a fair trial. Mass surveillance impinges on the untouchable "essence" of these rights. These deployments have happened de-

spite objections from Member States' dedicated Data Protection Authorities (DPAs)[93], the European Data Protection Supervisor (EDPS),[94] and in some cases, even their national Courts.[95] Due to the impermissible intrusive, undemocratic and violatory nature of biometric mass surveillance technologies in public spaces, these technologies should never be deployed or used. Furthermore, DPAs must be "provided with sufficient resources to carry out their tasks effectively."[96]

7.1 Recommendations: ban biometric mass surveillance

EDRi calls on the European Union to permanently stop all biometric processing in public and publicly-accessible spaces, wherever it has the effect or potential effect to establish mass surveillance. This call comprises of six actions. Whilst EDRi calls for the implementation of all measures below in order to eradicate biometric mass surveillance, these measures differ in the time-frames and efforts required for each specific action:

1. *EU Member States* immediately **halt all biometric processing that could amount to mass surveillance in public spaces**, ensuring that both current and future deployments are included. This should be supported by **a political debate by the European Council** on the fundamental rights impacts of biometric mass processing in Member States;

2. *EU Member States*, under the auspices of the European Data Protection Board (EDPB) and national Data Protection Authorities (DPAs), **publicly disclose all existing and planned activities and deployments** that fall within this remit;

3. *EU Member States* **cease all planned legislation which establishes biometric processing** that could lead to mass surveillance in public spaces. Instead, clear and foreseeable laws should only allow for targeted identification checks that are proportionate to the issues and context, and provide for effective remedies against abuse. DPAs can play a role by **advising national regulators and requesting action** from their national governments;

4. *The European Commission*, in particular Directorate-General (DG) HOME and with reference to DG RTD for the Horizon2020 Programme, ensure that funding given to Member States for biometric research or deployment is for activities

93 EDPB, *School renders Sweden's first GDPR fine* (2019) <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en>; the CNIL, *Experimentation de la reconnaissance faciale dans deux lycees* (2019) <https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position>

94 EDPS, *Facial Recognition: A Solution in Search of a Problem?* (2019) <https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en>

95 La Quadrature du Net et autres, Tribunal Administratif du Marseille, N.1901249 (2020) <https://www.laquadrature.net/wp-content/uploads/sites/8/2020/02/1090394890_1901249.pdf>

96 Fundamental Rights Review of EU data collection instruments and programmes, 112 <http://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf>

which are fully compliant with the Charter, including **immediately ceasing all funding for biometric processing programmes** which could contribute to mass surveillance in public spaces. All EU bodies who give operational support or advice to EU institutions, including but not limited to Europol, Frontex and the Fundamental Rights Agency (FRA), **ensure that Member States cannot use these technologies in a way which gives way to fundamental rights abuses**;

5. *The European Commission*, under the auspices of the EDPS's advisory role, **review and ex post facto evaluate on fundamental rights and data protection grounds all laws covering EU biometrics that contribute to or amount to mass surveillance** and, as appropriate, recast, repeal or provide appropriate guidance to Member States about safeguards;[97] and

6. *The European Commission* (in particular DGs GROW, CNECT and JUST as the Directorate-Generals leading the Commission's work on the White Paper on Artificial Intelligence (AI) and DG HOME in its capacity on borders) **implement, through legislative and non-legislative means** and if necessary, infringement proceedings and Court action, **an immediate and indefinite ban on biometric processing that leads to mass surveillance in public spaces**. This process must be done under the supervision and/or support of the European Data Protection Supervisor (EDPS), the European Data Protection Board (EDPB), the FRA and DPAs.

It is the role and responsibility of the European Union, in particular the European Commission, theCouncil of the EU and the European Parliament, with the support of the European Data Protection Board which also includes the European Data Protection Supervisor, the EU Fundamental Rights Agency (FRA), the national Data Protection Authorities (DPAs) of every EU Member State and any other oversight bodies, to determine the appropriate methods to ensure that biometric mass surveillance is comprehensively stopped and banned in law, and in practice, across the EU.

We further encourage Members of the European Parliament – in particular the intergroup on Artificial Intelligence & Digital; the Committee of the Regions (CoR); the European Economic & Social Committee (EESC) and all stakeholders who care about protecting the EU's fundamental rights, freedoms and values to join this call to ban biometric mass surveillance. We look to these public institutions to increase awareness of these issues in a variety of ways, for example proposing Parliamentary Resolutions and including calls for a ban in opinions and reports.

97 Many ofthe relevant laws are analysed in the report *Fundamental rights review of EU data collection instruments and programmes* <http://www.fondazionebrodolini.it/sites/default/files/final_report_0.pdf>

7.2 European Commission White Paper on AI

Within the European Commission's upcoming AI strategy, which was outlined in the Artificial Intelligence White Paper of 19 February 2020, the Commission proposed to include facial and biometric processing within a "high risk" regulatory framework for AI. The Commission should not attempt to "risk-assess" fundamental rights violations like biometric processing that leads to mass surveillance, just like it would not propose to "risk assess" genocide or torture. EDRi's position is that biometric processing in publicly-accessible spaces that leads to mass surveillance poses such a significant risk to the very essence of EU fundamental rights that it must be banned, and calls on DGs GROW, CONNECT and JUST to ensure that the Commission's position is compliant.

Indiscriminate, untargeted facial and biometric processing amounts to mass surveillance and is inherently associated with violations of rights to privacy, data protection, dignity, fundamental freedoms and justice. Whilst some uses of facial recognition or other biometric processing may use so-called artificial intelligence in the form of machine learning algorithms, the problem that we are specifically concerned about is the societal impact of any kind of mass surveillance, not the type of technology that is used to achieve the outcome.

Moreover, the Commission's AI strategy must appropriately regulate uses of AI that are outside the ban in a way that still complies with fundamental rights, including undertaking human rights impact assessments (HRIAs) and halting measures that unlawfully violate fundamental rights on any grounds. Whilst the scope of EDRi's call for a ban specifically relates to biometric mass surveillance, EDRi additionally strongly encourages the EU to cease funding for all biometric projects which are based on behavioural predictions, to assess the fundamental rights compliance of all funded projects, and to make those assessments public and subject to public debate both with civil society and with the European Parliament.

7.3 Preventing a digital dystopia

Data-hungry facial and other biometric processing that enable or contribute to mass surveillance are fundamentally at odds with the essence of human dignity, democratic society, fundamental rights and freedoms, protections for personal data, procedural rights, and the rule of law. The risks for increasing power imbalances, discrimination, racism, inequalities and authoritarian societal control in mass biometric processing are too high for any alleged "benefits" that the use of these technologies could ever conceivably bring. If the EU believes in the essence of fundamental rights, it has no choice but to ban the use of biometric processing that leads to mass surveillance in public spaces. EDRi's call for action is not a ceiling, but a floor for addressing biometric processing which violates the very core of European rights, freedoms and values.

"The use of biometric surveillance systems creates a dynamic where the powerful watch and the powerless are watched"

- European Digital Rights