ARTICLE 19

When bodies become data:
Biometric technologies and freedom of expression

2021

First published by ARTICLE 19 in April 2021

ARTICLE 19 works for a world where all people everywhere can freely express themselves and actively engage in public life without fear of discrimination. We do this by working on two interlocking freedoms, which set the foundation for all our work. The Freedom to Speak concerns everyone's right to express and disseminate opinions, ideas and information through any means, as well as to disagree from, and question power-holders. The Freedom to Know concerns the right to demand and receive information by powerholders for transparency good governance and sustainable development. When either of these freedoms comes under threat, by the failure of power-holders to adequately protect them, ARTICLE 19 speaks with one voice, through courts of law, through global and regional organisations, and through civil society wherever we are present.

ARTICLE 19
Free Word Centre
60 Farringdon Road
London EC1R 3GA UK

E: info@article19.org
W: www.article19.org
Tw: @article19org
Fb: facebook.com/article19org
ISBN: 978-1-910793-43-5
A19/LP/2021/001

Table of contents

Executive Summary **5**
Introduction **6**
Biometric technologies: background **8**
Key terminology 8
Reliability of some biometric technologies 8
The main uses and the dominant narratives behind the deployment of biometric technologies 9
International human rights standards and biometric technologies **11**
Applicable human right standards 11
Human rights standards on biometric technologies 13
Human rights responsibilities of the private sector 15
Biometric technologies and the right to freedom of expression and information **16**
Biometric technologies and human rights: overall challenges 16
Data collection, storage and retention 16
Possible security breaches 16
'Black box' problem 17
Scale 17
Inadequate or missing national legal frameworks 17
Necessity and proportionality 18
Lack of remedies in cases of human rights violations 18
Biometric technologies and challenges to freedom of expression and information 18
Chilling effect of mass surveillance on freedom of expression 18
Impact on the right to freedom of expression of specific categories of individuals 19
Need for transparency and access to information 19
Biometric technologies and freedom of expression: case studies **21**
Facial recognition 21
Purposes and usage of facial recognition technologies 21
Challenges raised by facial recognition to the exercise of human rights 22
Challenges raised by facial recognition to freedom of expression and information 24
Emotion recognition 25
Purposes and usage of emotion recognition technologies 25
Effectiveness of emotion recognition technologies 26
Challenges raised by emotion recognition technologies to human rights 26
Challenges raised by the use of emotion recognition technologies to people's ability to exercise their freedom of expression 27
ARTICLE 19's recommendations **28**
Endnotes **32**

Executive summary

In this policy, ARTICLE 19 outlines its position on the effects that the development and deployment of biometric technologies have on the right to freedom of expression.

This policy is motivated by concerns about the rapid and increased use of biometric technologies not only by the private sector but also by public authorities. Biometric technologies are being used to analyse the way people act, look, and express themselves in public and private spheres. Their use ranges from border patrol to unlocking a smartphone, but one thing is clear: their use is being normalised. These technologies have the power to change the way people act in public spaces and therefore risk the very existence of civic space, an essential pillar of democracy, that allows public participation and exercise of human rights.

State or private actors who design, develop and deploy biometric technologies must do so using a human rights approach in order to protect individuals' fundamental rights. In particular, ARTICLE 19 highlights the following concerns:

- Increased mass surveillance of public spaces using biometric technologies, including facial recognition and emotion recognition, will undoubtedly create a severe chilling effect on freedom of expression and public participation.
- States and the private sector are developing and deploying biometric technologies without considering the harm they may cause to people's lives and how they might prevent people's ability to exercise their human rights. This is very concerning as they can use these types of technologies in ways that are highly intrusive, violate the rights to right to freedom of expression and privacy and do not adequately protect personal data.
- There is a severe lack of accountability. State or private actors have not put in place effective mechanisms for potential victims to claim remedies for violations of their rights. If, for example, people face discrimination as a result of the use of face recognition, it is unclear how this issue would be addressed and how and if any remedies will be provided.
- Lastly, the availability of a particular biometric technology (or any technology) should not automatically justify its use. The design of the technologies means they are ripe for abuse, open to security breaches and indicate several biases. Rather than placing technology at the service of human beings or designing solutions that solve existing problems, the push to develop tools and products for their own sake is fundamentally flawed.

For these reasons, ARTICLE 19 warns against the use of biometric technologies, especially on national security and counterterrorism grounds, without a sufficient legislative framework to protect human rights. We consider that a human rights-based

approach ought to be embedded at the start of the design and development of any technology. Therefore, we call for a moratorium on the development and deployment of all biometric technologies by both States and private actors until they can ensure the full protection of freedom of expression and full compliance with international human rights standards.

This policy brief is divided into five parts. First, we outline key background information and terminology concerning biometric technology. Second, we outline all relevant international standards on freedom of expression applicable to biometric technology. This is followed by a section on how the use and abuse of these technologies obstruct people from exercising their human rights with a particular focus on how they prevent people from exercising their right to freedom of expression and information. We then provide two cases studies - one on how facial recognition limits freedom of expression and the other on how emotion recognition limits freedom of expression. Finally, we make a list of comprehensive recommendations directed at States, private companies, and all other relevant stakeholders.

Summary of recommendations:

1. States should ban biometric mass surveillance
2. States should ban the design, development and use of emotion recognition technologies
3. Public and private actors who design, develop and use biometric technologies should respect the principles of legitimacy, proportionality and necessity
4. States should set an adequate legislative framework for the design, development and use of biometric technologies
5. Government authorities must ensure that the design, development and use of biometric technologies are subject to transparency and open and public debate
6. Transparency requirements for the sector should be imposed and thoroughly implemented by both public and private sectors
7. States should guarantee accountability and access to remedies for human rights violations arising from biometric technologies
8. The private sector should design, develop and deploy biometric systems in accordance with human rights standards.

Introduction

Around the world, governments and private actors who use identification and verification systems increasingly rely on biometric data - from fingerprints and DNA samples to more advanced biometric technologies that aim to identify persons on the basis of their physical traits, behaviour or activities.[1] Public and private actors now use these technologies in various settings for the real-time measurement and analysis of the way people look, sound, move and behave. These technologies are increasingly applied in areas such as crime and border control, advertising or marketing;[2] they are a popular tool to unlock a smartphone, access an online bank account or even access physical and other online spaces.[3] Their massive use is, however, not necessarily limited to the identification of people. It also results in profiling and categorising people based on age, gender, skin colour, surveilling what they are doing, with whom, how they are feeling and even how they are likely to behave in the future.

Biometric technologies have rapidly developed in recent years due to two main factors. The first is the availability of an **unprecedented number of large datasets** – collected mostly by private actors based on ever more data-driven business models and supported by an alarming counter-terrorism and public security narratives. The second factor is the increasing availability, at lower prices, of **machine learning**, both in terms of hardware (computer power and infrastructure) and pure software (including libraries, more machine learning talent and funding). Both factors are strongly interrelated as the latter needs the former to work. These advances have enabled a vast diffusion of surveillance systems and a transition from a world where tracking and identification were the exception, to a world where they are becoming the norm.

While the technology has evolved and become increasingly popular, the relevant legislative frameworks have not evolved at the same pace. Although many countries have issued specific regulatory frameworks for the use of 'first generation' biometric technologies, the same cannot be said about more recently developed ones, a majority of which operate without specific legal basis. This is highly problematic because the misuse/abuse of biometric technologies impacts people's lives in several ways. These technologies are especially intrusive and their deployment and use often violate the human rights to privacy and data protection,[4] human dignity,[5] non-discrimination,[6] self-determination and the right to access an effective remedy.

The ever increasing, pervasive and often invisible use of biometrics technologies by public authorities and private entities, coupled with their ability to identify and track people and behaviours, also prevents people from exercising their right to freedom of expression, particularly the ability to remain anonymous. It has also damaged civic space: the place where individuals realise their rights, participate, express, assemble, and inform themselves. As civic space is a fundamental pillar of democracy, the diffuse deployment and use of biometric technologies puts at risk its very existence.[7] There is also a serious lack of transparency about who is developing and deploying these technologies, the

manner in which they do so, and why these technologies are being developed. This precludes a public and open debate about their use by the public and private sectors.

Recently, the **COVID-19 pandemic** has reinforced calls for technological solutionism and provided additional impetus for public and private actors to further develop and deploy biometric technologies as 'core' tools in the pandemic measures.[8] These include various quarantine or contact tracing apps,[9] as well as the police use of surveillance helmets to scan people for COVID-19 fever as they walk past in public spaces.[10] Worryingly, both public and private actors have pushed for a narrative that pits human rights against public health,[11] and are pushing populations to accept an unprecedented level of mass surveillance. While measures to protect people from COVID-19 are extremely important and could be simplified through the use of biometric technologies, the technologies are unlikely to be the panacea they are often claimed to be. In any case, due to the fact that they can be used to intrude into people's private lives, the use of these technologies should always be kept in check and comply with international standards, and never be normalised.

ARTICLE 19 considers important to contribute to the current debates about whether the tendency to abuse biometrics could be mitigated or whether state and private bodies should be banned from using these technologies altogether. In this policy document, we examine how the misuse/abuse of biometric technologies blocks people from fully exercising their right to freedom of expression and information and make recommendations to States, private actors and all other relevant stakeholders on how to protect and promote freedom of expression.

The structure of this policy paper is as follows:

- First, we set out some basic definitions, terminologies and concepts around the use of biometric technologies
- Second, we outline the international human rights standards that apply to the use of these technologies
- Third, we assess the impact of biometric technologies on the right to freedom of expression
- Fourth, we examine two specific case studies of biometrics and freedom of expression - one on facial recognition and one on emotion recognition
- Finally, we make recommendations for States, private actors, and other relevant stakeholders about how to guarantee the protection of freedom of expression in the design, development and deployment of biometric technologies.

Our recommendations for States, private actors and all other stakeholders come together with a heartfelt call not to subtract from public debate one of the most important battles to define freedom of expression and the very existence of civic space for our generation and those to come.

Biometric technologies: background

Key terminology

The term '**biometrics**' commonly describes the physiological and behavioural characteristics of individuals. This could be, among others, fingerprints, voice, face, retina and iris patterns, hand geometry, gait or DNA profiles.

Biometric data has been defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data."[12] Biometric data changes irrevocably the relation between body and identity, because it makes the characteristics of the human body 'machine-readable' and subject to further use.[13]

The term **biometric technology** then refers to a variety of technologies that measure and analyse unique human characteristics such as DNA, fingerprints, voice patterns, hand measurements, eye retinas or irises, cardiac signatures.[14] More recently, biometric technologies include, *inter alia*, multimodal biometrics, behavioural biometrics, dynamic face recognition, remote iris recognition, and several other applications at different stages of development.[15]

The term **face recognition/facial recognition** falls within a wider category of biometric technologies and can be defined as "automatic processing of digital images which contain the faces of individuals for authentication, identification or categorisation of those individuals."[16]

The term **emotion recognition** is a biometric technology which uses machine learning in an attempt to identify individuals' emotional states and sort them into discrete categories such as anger, surprise, fear, happiness, etc. Input data can include individuals' faces, body movements, vocal tone, spoken or typed words, and physiological signals (e.g., heart rate, blood pressure, breathing rate, body language or voice tone).[17]

Reliability of some biometric technologies

The accuracy and reliability of applications of biometric technologies for emotion and behaviour recognition are yet to be proven. A vast amount of scientific studies warn that facial expressions and other external behaviours are not reliable indicators of inner emotional states.[18] They warn that inaccuracies lead to discrimination of racial, ethnic or other minorities and also highlight the racist assumptions that form basis of these technologies.[19]

For instance, many of these technologies and applications rely on the historical perception inaugurated by studies on phenotypes, inspired by race classification and racist assumptions (facial angle, cranioscopy/phrenology, physiognomy, anthropometry).[20] Such techniques were created to establish the so-called "scientific racism" applied to the colonial world.[21] Although the scientific validity of such methods were never proved, the application of those techniques marked the mind frame for the evolution of this line of study, mainly in application for profiling, classifying and identifying stereotypes to serve in criminal anthropology and eugenic parameters.[22] The social history of biometric technologies is thus fundamental to understand the challenges related to how they are used today. Therefore, even if accuracy is improved, active discrimination and the arising legal issues would remain unresolved.

This means that the acceptability of the deployment of biometrics has to be lashed firmly to a balancing exercise that considers, on the one hand, the legitimate interest to the use of the technology, and, on the other hand, the need to guarantee human rights protection.

The main uses and the dominant narratives behind the deployment of biometric technologies

Governments and private actors currently use biometric technologies in a number of ways, claiming that they will achieve various objectives. The most prominent claims include:

- Protection of **national security, anti-terrorism measures and crime prevention and control** have been used to justify the deployment of biometric technologies in various settings over the past two decades, and ranging from border controls and management[23] to national identification systems[24] Beyond security and safety narratives, law enforcement agencies have been using facial recognition technology as a tool that has the potential to help prevent and detect crime, preserve public safety and prosecute perpetrators;[25] but also for prevention of fraud and theft or following movements of minorities.[26]
- Biometric technologies have been also used by public authorities for management and access to various state functions and the **delivery of public services**,[27] such as e-health systems and electoral registers.[28] They are also relied on in private or privately led uses, such as the **development of "smart cities" projects**, public transport, access to schools or access to physical and online spaces.[29]

The deployment of biometric technologies is usually justified by referring to a number of advantages they are supposed to deliver. These include fast and frictionless access,

cost saving solutions, accuracy and reliability, enhanced security, improved welfare provisions. However, most of these advantages come unproven, or the assessment does not take into due account the vast trade-offs in terms of human rights protection.

Furthermore, we have assisted to the wide use of the rhetoric that the availability of a technology is enough to justify its usage. We should strongly resist this approach. The design, development, and use of biometric technologies cannot be assumed to be neutral. At the technical level, biometrics make numerous assumptions; at institutional level, they are used in fundamentally discriminatory ways that exacerbate social disadvantages and historical discrimination. Overarching, biometric technologies function as sociotechnical systems that reflect values and assumptions, which, as discussed in this policy brief, are far away, if not totally incompatible with human rights protection.[30]

International human rights standards and biometric technologies

Applicable human right standards

There are no explicit international standards that deal with biometric technologies; however, their deployment and use affect people's ability to exercise a number of human rights. In particular:

- The **right to freedom of expression**, protected by Article 19 of the Universal Declaration of Human Rights (UDHR),[31] and given legal force through Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[32] as well as in regional human rights treaties.[33] Under international human rights standards, restrictions on the right to freedom of expression are permitted only under very specific circumstances (so called three-part test); all restrictions must be strictly and narrowly tailored and may not put the right itself in jeopardy.[34]
- The **right of access to information** is recognised as an element of the right freedom of expression. The UN Human Rights Committee, a body tasked with interpreting the ICCPR (HR Committee), interpreted the scope and limits of the right to information in 2011, stating that Article 19 of the ICCPR ensures the right to information held by public bodies. It requires that States proactively disseminate information in the public interest and that the access is "easy, prompt, effective and practical."[35] The Committee also stipulated that States must enact "necessary procedures" such as legislation to give effect to the right to information and that fees for access must be limited, responses to requests must be timely, authorities must provide explanations for withholding information, and States need to establish appeals mechanisms."[36]
- The **right to freedom of peaceful assembly** is guaranteed in Article 20 para 1 of the UDHR and given force in Article 21 of the ICCPR, Article 5(d) of the Convention on the Elimination of Racial Discrimination[37] and in regional treaties.[38] Under these standards, requirements for a permissible restriction must comply with the same three-part test as for the restrictions on the right to freedom of expression.[39]
- The **right to privacy** is guaranteed by Article 12 of the UDHR and Article 17 of the ICCPR and in regional treaties.[40] Under these standards, privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including governments, companies, and other individuals. The right to privacy is commonly recognised as a core right that underpins human dignity and other values. Restrictions on privacy must also meet the requirements of the three-part test.[41]

- The **right to non-discrimination and the right to equality** is protected by Article 2 and Article 7 UDHR, and given legal force through Article 2 and 26 of the ICCPR, Article 2(2) of the International Covenant of the Economic, Social and Cultural Rights (ICESCR), as well as regional treaties and instruments.[42] The right to equality implies that all persons are to be given "equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."[43]

Freedom of expression and privacy are mutually reinforcing rights; all the more so in the digital age.[44] Privacy is a prerequisite to the exercise of freedom of expression: without it, individuals lack the space to think, speak and develop their voice. It follows that, to the extent that States develop or use biometrics in a manner that interferes with the right to privacy, that use must be subject to the three-part test of legality, necessity and proportionality.

Additionally, the protection of **personal data** (data protection) is recognised by the HR Committee as a fundamental part of privacy.[45] The 1990 Resolution of the UN General Assembly on guidelines for the data protection of personal information held in computer databases[46] sets out 6 basic principles of data protection based on fair information practices. On a regional level, the protection of personal data is also guaranteed in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[47] under the EU Charter,[48] under the African Union Convention on Cyber Security and Personal Data Protection (AU Cybercrime Convention)[49] and under the Principles on Privacy and Personal Data Protection of the Organisation of American States.[50]

International human rights law also recognises that individuals who want to know if and why they have been subject to the use of biometric technologies by public administration have the right to do so under data protection law. Among these rights, there is the right to be informed about the collection and use of their person data, which leads to a variety of information obligations by the controller.[51] In General Comment 16, the HR Committee noted that the right is necessary in order to ensure respect of the right to privacy.[52] This right has been widely incorporated into international law, as well as in major regional agreements on data protection.[53] Under the General Data Protection Regulation (GDPR), every individual has a strong right to be informed and it differentiates between two cases: on the one hand, if personal data is directly obtained from the data subject (Article 13) and, on the other hand, if this is not the case (Article 14).[54]

The importance of ensuring strong safeguards to prevent unlawful access to data and transparency has been stressed in the European Union by the Fundamental Rights Agency (FRA) with particular reference to the collection of personal data including fingerprints of asylum and visa applicants, as well as migrants in an irregular

situation.[55] Some States have also established the protection of these rights and privacy safeguards in their national legislation.[56]

International human rights bodies have also moved towards recognising a **right to anonymity** as an important aspect of the right to freedom of expression and privacy. This has implications for biometric technologies used to identify individuals in their homes and in public spaces. Hence, state interference with anonymity should be subject to the three-part test of legality, necessity, and proportionality, as is any other interference with this right.[57]

Human rights standards on biometric technologies

Although there are no international standards that deal explicitly with biometric technologies, there is an emerging body of standards that is relevant for their development and deployment.

First, human rights bodies are increasingly recognising and acknowledging the ways in which new forms of data-processing impede people's ability to exercise their human rights. With respect to profiling, for example, which may involve the use of biometric systems to derive, infer or predict information about individuals for the purpose of evaluating or assessing some aspect about them, the UN Human Rights Council noted with concern in March 2017 that:

> Automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights.[58]

Second, specifically in relation to biometric data:

The Council of Europe Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (the Convention 108+) provides that biometric data uniquely identifying a person shall only be allowed where appropriate safeguards are enshrined in law, complementing those of the Convention 108.[59]

The EU General Data Protection Regulation (GDPR) prohibits the processing of biometric data for the purpose of uniquely identifying a natural person subject to limited exceptions.[60] In addition, the GDPR treats biometric data used for identification purposes as "special category data," meaning it is considered more sensitive and in need of more protection. The same approach is adopted in the Standards for Personal Data Protection for Ibero-American States.[61]

The AU Cybercrime Convention requires preliminary authorisation from the national data protection authority for the processing of personal data involving biometric data.[62]

Other international instruments provide useful guides about how to assess the use of biometric technologies and their impact on people's ability to exercise their human rights. For instance, the UN High Commissioner for Human Rights in his report on the right to privacy in the digital age highlighted the concerns over the use of biometric data, its potential to be "gravely abused" and States embarking on biometrics-based projects without "adequate legal and procedural safeguards in place."[63] The report recommends that States, *inter alia*:

> Ensure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim.[64]

Moreover, three human rights mandates have already warned about biometrics systems:

In 2019, the UN Special Rapporteur on Freedom of Association and Assembly declared in his 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."[65]

- The UN Special Rapporteur on the Right to Privacy has called into question the necessity and proportionality of biometric systems.[66]
- The UN Special Rapporteur on Freedom of Expression raised similar concerns about the impact of biometric systems on human rights defenders, journalists, politicians and UN investigators.[67]

The case law of international bodies and regional and national courts also provides general indications about the standards to be applied while using biometric technologies. In particular, the European Court of Human Rights (European Court) has highlighted the need to strike a balance between the protection of fundamental rights, and the development of new technologies, and has 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."[68]

A partially different approach seemed to be taken in the field of counter-terrorism. In 2017, the UN Security Council decided that States shall develop and implement systems to collect and share biometric data for purposes of counter-terrorism.[69] Similarly, the 2018 Addendum to the Madrid Guiding Principles note the usefulness of biometrics data.[70] As a result, biometric systems are considered a legitimate tool for the identification of terrorist suspects.

Nevertheless, even when the purpose is to counter terrorism, the use of biometric technologies must comply with international standards, and in particular with the principles of necessity and proportionality. The UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism (UN Compendium) could be considered a first step towards a more human rights centric approach, but it is not a sufficiently adequate framework.[71]

Human rights responsibilities of the private sector

While international human rights law places obligations on States to protect, promote and respect human rights, it is widely recognised that the private sector also has a responsibility to respect human rights.[72]

The Guiding Principles on Business and Human Rights (the Guiding Principles) provide a starting point for articulating the role of the private sector in protecting human rights on the Internet.[73] They recognise the responsibility of business enterprises to respect human rights, independent of state obligations or the implementation of those obligations, and recommend several measures that companies should adopt.[74] These include incorporating human rights safeguards by design in order to mitigate adverse impacts on people and communities, building leverage and acting collectively in order to strengthen their power vis-a-vis government authorities; and making remedies available where adverse human rights impacts are created.

Various stakeholders have called for regulation. In a limited extent, this is true also for tech companies, which after responding to initial calls for adopting standards on 'ethical' or 'trustworthy' biometric technologies, started to acknowledge that a step further was needed, and have called for regulation too. However, both the 'ethical' and the regulatory proposals made by tech companies have been rarely, if ever, adequate. Moreover, these are calls for soft measures rather than calls for adequate frameworks of human rights' protection in biometrics.[75]

Finally, there is growing recognition that technical standards and protocols should be grounded in a human rights approach, as the former can have a substantial impact on the exercise of the latter.[76] However, despite this increased recognition, human rights are neither explicitly nor adequately referred to in the policy processes of many technical or business organisations, although these actors are fast becoming the gateways to and facilitators of the exercise of freedom of expression and freedom of assembly, since they develop the majority of biometric technologies' systems. While initiatives such as the Google' Artificial Intelligence Principles[77] can be read as a step in this direction; they have nonetheless demonstrated many shortfalls and, so far, they have been unable to ensure sufficient levels of companies' transparency and accountability.

Biometric technologies and the right to freedom of expression and information

Biometric technologies and human rights: overall challenges

Prior to discussing the challenges brought by the misuse or abuse of biometric technologies to the exercise of the right to freedom of expression and information, ARTICLE 19 highlights the following problems that these technologies pose from a human rights perspective overall:

Data collection, storage and retention

The development and deployment of biometric technologies imply the collection and generation of large amounts of sensitive personal data. Biometric data are a special category of personal data which, because of their capacity to reveal intimate information about a person (fingerprints, eye scans, racial or ethnic origin, sex and so on,), require additional safeguards and enhanced protection. From the start, then, biometric technology is designed to be very invasive. Moreover, datasets are often built through problematic methods of collection (for example, data samples can be unrepresentative of the population at large) and hold biases that reflect existing patterns of societal stereotyping.[78]

Equally problematic is the diffuse practice of indiscriminate retention of biometric data that does not meet the necessity and proportionality test.[79] In other words, data processors often keep the biometric data for longer than they need based on the purpose of holding the data.

Furthermore, these massive databases can easily be re-purposed by state or private actors for purposes other than which they were originally intended. This raises the issue of 'mission creep,' or the potential to expand the application of such technologies' to collect data and/or execute functions that were not originally approved. There is already evidence of biometric databases that were created for a single purpose have been re-purposed or abused for another purpose.[80] In these cases, even if people consented to the use of their biometric data for the initial purpose, their consent does not cover the repurposing, and this repurposing must then be considered illegal.

Possible security breaches

Security breaches of databases are difficult to detect and extremely costly to repair. Even more difficult is for individuals to seek redress when they suffer harm from such a breach. Indeed, biometric data are not like passwords that can be changed in case of leaks; on the contrary, they can be used to identify and track an individual for life. Security risks are higher in case of large and centralised databases and will particularly

affect those communities who are already marginalised; for this reason, centralised databases should be considered only in case of absolute need and only when there is no viable alternative available.[81]

Finally, security risks are higher in countries where the tech industry and the data security infrastructure do not exist or are insufficiently developed. In this context of distrust, it becomes deeply worrisome that either the government or other actors retain individuals' biometric data.

'Black box' problem

Newer applications of biometric technologies are increasingly based on machine learning which raises the 'black box' problem.[82] The inscrutability of machine learning processes and systems is a fundamental challenge to accountability and redress in the context of automated decision-making. Given a significant automation bias in favour of machine-made decisions, along with imperfect and often clunky technical systems, profiling and matching become difficult or impossible to challenge particularly when the logic and assumptions on which decisions are made are not clear. As a consequence, it becomes difficult, if not impossible, for courts to judge the veracity of evidential claims.

Scale

Biometric technologies are currently deployed at an unprecedented scale, potentially leading to a state of mass surveillance in various areas of the world. From airports to public squares, from thermal cameras to fingers' vein identification systems, the use of these technologies to identify and monitor individuals is becoming increasingly widespread.[83]

Inadequate or missing national legal frameworks

Inadequate or non-existent national legal frameworks for the development and deployment of biometric technologies is a serious problem. Data protection legislation (if they exist in the first place), although necessary, might not be sufficient to cope with all relevant problems. In order to do so, they have to contain clear rules on, among others, consent, lawfulness of processing, purpose limitation. In addition, various data protection frameworks provide for exceptions when it comes to the processing of personal data for law enforcement purposes. These exceptions are often shaped in vague and broad terms, without sufficient guarantees for the protection of individuals' data. A proper legislative framework, compliant with international standards, is needed for the development and use of biometric technologies by both public as well as private actors.

Necessity and proportionality

States and private actors are developing and deploying biometric technologies for an ever-increasing list of purposes. The availability of the technology is often considered a sufficient reason for its use, without an adequate assessment of the legitimacy of the aim. The development and deployment of these technologies for purposes that undermine human dignity, for example for total digital monitoring, humiliation or manipulation, should never be allowed.[84] Even when a legitimate purpose for the use of biometrics is identified, its deployment does not always meet a narrowly constructed test of necessity and proportionality: the technology has to be absolutely necessary to achieve the scope and there should be no other less invasive means to do so. If this test is not passed, the use of the technology should not be allowed, irrespective of its availability or allure.[85]

Lack of remedies in cases of human rights violations

Neither public nor private actors dealing with biometric technologies have put in place effective remedies in case of violations of human rights. For instance, if the use of biometric technology leads to a discriminatory result, it is not clear how such a situation will be addressed. Equally, if the police use biometric technology to track individuals engaging in political, religious, or other categories of protected expression, it is not clear what would be the remedy at disposal for those individuals. In any case, a precondition to the right of an effective remedy is that people are aware that their biometric data is being processed or that a decision concerning them has been taken based on the use of biometric technologies. This is not the case in a vast majority of situations.

Biometric technologies and challenges to freedom of expression and information

Some of the challenges posed by the use of biometric technologies on people's ability to exercise their rights to freedom of expression and information are similar to the challenges posed by previous technologies. However, certain challenges originate from specific features of biometrics. These include the following:

Chilling effect of mass surveillance on freedom of expression

Although human rights law evolved to understand that the protections against unlawful or arbitrary mass surveillance are primarily guaranteed by the right to privacy,[86] there is a growing recognition that mass surveillance has a chilling effect on freedom of expression as well.[87] If biometric technologies are used for identification or profiling purposes in public spaces, such as the use of facial recognition technologies to process facial images captured by video cameras on streets, squares, subways, stadiums or concert halls, they negate individuals' ability to confidently communicate anonymously,

and have anonymity when moving and behaving in public spaces. Similarly, they directly impede the way in which NGOs operate with regards to the protection of their sources as well as their "watchdog" function.[88] Studies show that the awareness of being watched and tracked might lead people not to join public assemblies, or not to participate in social and cultural life, and not to freely express their thoughts, conscience and religious beliefs in public spaces.[89]

Impact on the right to freedom of expression of specific categories of individuals

The use of biometric technologies can have a more severe impact on the right to freedom of expression of certain groups of people who might be targeted for their exercise of this right, or on minorities. For example, journalists could be discouraged in conducting investigations or establishing contacts with their sources of information if they know that they could be monitored/spied upon and identified by biometric technologies in public or private spaces.[90] The fear of being tracked and watched can have a strong chilling effect on them; this, in turn preventing quality journalism and investigative reporting, frustrating the role that media play in our societies. Activists and political opponents might have similar fears and thus the same incentives to self-censorship. For example, they can be dissuaded from exercising their right to protest if, as a consequence of the use of biometric technologies by the State, they will be attributed specific classifications, such as 'habitual protestors' or similar.[91]

Need for transparency and access to information

The widespread deployment of biometric technologies and the set-up of overbroad databases coupled with an overall lack of transparency about their deployment and use also raise challenges for individuals' right to access information. When governments collect and store massive amounts of biometric data, it is crucial that the public also has a right to know what the government is doing with that information. This is a particular problem when the public or private actors deploy the technologies for identification and monitoring in public spaces.

There is no sufficient accessible information about who is developing biometric technologies, what kind of technology is being developed, who is deploying them, how, and for which purposes. It is also unknown whether developers and sellers carry out any kind of due diligence to evaluate the human rights record of purchasers.[92]

State and private actors are close collaborators in the markets for biometric technologies. However, the content and terms of public-private partnerships, and public contracts (through which public authorities buy the technologies from the industry), are not made public. In general, States fail to disclose their relationships with developers, including the criteria for bids' assessment and contract assignments. This opaque and secretive environment leads to the biometrics technologies being bought and used

without due public scrutiny, with weak procedural safeguards and ineffective oversight. In a similar vein, public authorities dealing with biometric technologies appear not to conduct adequate impact or risk assessments, which are both important components of accountability.[93]

Freedom of information or right to information laws are powerful legal tools that individuals, journalists and activists can use to improve government transparency and to understand the government's use of biometric data.[94] However, attempts to access information held by public bodies on the use of biometric technologies through these laws have proved to be challenging.[95] Considering the vast numbers of people from whom biometric data is gathered, it seems undisputed that the general public has an interest in the systems designed to store and manipulate significant quantities of such data.[96] Regardless, public bodies often fail to proactively publish information about such identification systems. Frequently, this information has only been released after pursuing a judicial appeal that challenges a denial of their request. Judicial appeals are typically long and costly in most jurisdictions, and requesters, including journalists, scientists and activists, often give up.

It should also be noted that some initiatives have addressed the lack of transparency over the use of biometric technologies by recognising that policy needs must be reconciled with ethical concerns and that implementation of such policies should be based on openness and transparency.[97]

Biometric technologies and freedom of expression: case studies

Facial recognition

Purposes and usage of facial recognition technologies

Facial recognition is the automatic processing of digital images which contain the faces of individuals for three main purposes:

- **Verification**, which is the comparison of two biometric templates to determine if the person shown in the two templates is the same (one-to-one comparison).
- **Identification**, which implies the comparison of a person's template with several templates in a database to verify if they are in the database (one-to-many comparison). When facial recognition is used live for this purpose, it is also referred to as 'automated or live facial recognition' (AFR or LFR). Although both one-to-one authentication and one-to-many come with problems,[98] the use of facial recognition for one-to-many identification purposes obstructs people from exercising their right to freedom of expression the most.
- **Categorisation**, which is used to profile people based on their personal characteristics, such as sex, age, and ethnic origin.[99]

The deployment of facial recognition has steadily increased in recent years. Various governments and municipalities around the world are discussing and implementing rules that foreshadow the massive deployment of facial recognition in public spaces for law enforcement purposes.[100] In some countries, the public security rhetoric is widely used to justify this ever-increasing surveillance of public spaces..[101]

Private actors use facial recognition for various purposes as well. For instance, thousands of retailers are using facial recognition to check customers in their stores against images of known shoplifters.[102] Some have gone further and used facial recognition to monitor customers' reactions to items in the store,[103] or as a system for customers to make purchases.[104] Live entertainment companies use facial recognition to identify ticket owners and facilitate their access to services or parts of venues. Transportation companies have deployed facial recognition systems in advertising panels located at subway stations in order to identify people's reactions to the advertisements (happy, dissatisfied, surprised and neutral) and supposedly link it with their physiological characteristics (age and gender).[105] Additionally, they use facial recognition as a safeguard against fraud and to check the identity of their drivers.[106] As mentioned earlier, a number of smartphone producers allow users to unlock their phone using a facial recognition feature.[107]

On the other hand, at a regional level, a number of municipalities are moving in the opposite direction and banning the use of facial recognition for certain purposes.[108] Similarly, a number of developers of facial recognition technologies recently took steps (albeit limited), to limit or suspend its development and deployment.[109] The scope of these commitments is not yet clear, but these moves can be seen as a signal of the mounting pressures to limit or ban the indiscriminate use of facial recognition for law enforcement purposes. Nevertheless, very few voices appear to raise these concerns, and they do not attribute equal weight to the dangers of purely private sector deployment of facial detection systems. This lack of concern is in stark contrast with the ever-increasing use of facial recognition by private actors, which spans from narrow and localised uses to widely deployed ones.[110]

The **COVID-19 pandemic** has drawn greater attention to facial recognition technologies. Developers have taken advantage of this public health emergency to push for new and broader uses of facial recognition by public and private actors alike, and governments are increasingly deploying this technology for monitoring purposes, to enforce quarantines, or to track infection chains.[111] The push towards the use of facial recognition technologies is so high that developers are already trying to overcome technical challenges raised by the mandatory or recommended use of face masks as a health measure to fight the pandemic. For instance, a few companies have started to develop 'periocular' recognition algorithms that detect and recognise faces based only on the eye region between cheekbones and eyebrows.[112] Still, facial recognition technology is being proposed as a solution for COVID-19, without any proof that such surveillance can actually deliver against its stated objective, or even work properly when people wear masks. Rather, these initiatives appear as part of a larger effort to establish an ever-expanding surveillance infrastructure under the guise of a pandemic response.[113]

Challenges raised by facial recognition to the exercise of human rights

All uses of facial recognition technology – whether by the public or private sector – have an impact on people's ability to exercise their human rights. Sometimes, facial recognition is more dangerous when used by private actors. Consumers are often convinced to embrace these technologies in their private sphere (home, relationships with family and friends or work) for ever more futile objectives, none of which are justified or proportionate to the violation of human rights that comes with the use of facial recognition.

Many concerns about the deployment and use of facial recognition are similar to those listed earlier for other biometric technologies. This technology is often deployed without a legal basis, in the absence of any specific legislative framework or any adequate safeguard for human rights and without previous public consultation. However, due to its specific features, facial recognition technologies raise specific challenges to the exercise of human rights and freedom of expression. This is because facial recognition has two particularities as compared to other biometric data. On the one hand, it can

be collected without a person being aware of it; on the other hand, it can mark out protected characteristics under international law (race, religion, sex and others).

The following key concerns should be noted:

- **Consent**: Facial recognition technologies do not need contact, nor an active behaviour from the target. For this reason, actors using facial recognition can easily subject targets to facial recognition without their knowledge or consent.[114] For example, Facebook, one of the first developers of facial recognition technologies, has vastly used users' face images to train its face recognition system, without informing them or asking for their consent.[115] Even when the use of face recognition is uncovered, it can be difficult to establish when valid consent is provided. Studies have argued that the use of Facebook's face recognition would in any case fail the consent standards by obscuring risk and corroding collective autonomy.[116]

- **Lack of transparency**: Although the lack of transparency is a general concern for the use of biometric technologies, facial recognition raises even greater concerns due to its heightened invasiveness. As explained earlier, a face image can be captured without the target being aware of it. This, coupled with lack of transparency about deployment by both public and private actors, leaves individuals in the dark, and totally exposed to misuses and abuses.

- **Accuracy**: Similar to other biometric technologies, facial recognition is based on a statistical estimation of correspondence between the compared elements; therefore, it is intrinsically fallible. Numerous studies demonstrate that facial recognition fails in terms of accuracy, particularly for underrepresented or historically disadvantaged groups.[117] For facial recognition to be free from bias, data quality and the comprehensiveness of the training databases are essential. If data quality is not ensured, or if training databases are over or under representative of certain characteristics, facial recognition is very far from reliable.[118] This is, especially problematic in cases of racial bias.[119] The accuracy of facial recognition systems is tremendously important because mistaken identity is more than an inconvenience and can result in severe consequences. For instance, a false negative in a one-to-one search might not allow an individual to access services or premises. A false positive in a one-to-many search puts an incorrect match on a list of candidates that warrant further scrutiny, or that are labelled in a certain way, and once this happens, it appears difficult, if not impossible, to reverse the situation.[120]

- **Little to no oversight**: Apart from a few exceptions, law enforcement agencies have little to no oversight of the use of facial recognition in various countries. In most places, there is nothing explicitly preventing authorities from using facial recognition on live camera feeds, turning passers-by into unknowing

participants of a virtual police line-up; and there are no rules about the retention of data collected through the use of facial recognition. These concerns are equally relevant when assessing how private actors use facial recognition: in the absence of appropriate oversight, companies deploy facial recognition for purposes and in ways that violate human rights standards.

- **Lack of standards**: Standards and best practices for the deployment of facial recognition are still in the process of being created.[121] There have also been calls for a statutory code of conduct.[122] Despite the lack of standards, facial recognition technology continues to be used in both public and commercial spaces across the world. This dangerous vacuum cannot simply be filled by calls for ethical use: ethical concerns must be addressed by an adequate regulatory framework that is compliant with international human rights standards.[123]

- **Dual use**: A vast majority of facial recognition systems marketed by private actors can be used for purposes that are different from the one they have been designed or provided for. In other words, the potential for abuse is staggering. The lack of a regulatory framework that provides guarantees against dual use, attributes liability and provides for remedies if it happens dramatically amplifies the risks.

- **Lack of necessity and proportionality**: Many use-cases of facial recognition technologies have already been considered as failing the necessity and proportionality test. Among others, the use in schools, with the purpose of controlling students' access has been condemned by data protection authorities and courts alike.[124]

Challenges raised by facial recognition to freedom of expression and information

From a freedom of expression perspective, the deployment and use of facial recognition technology raises the following additional problems:

- **Right to remain anonymous**: The use of facial recognition, and especially live facial recognition, in public spaces is an evident challenge to anonymity. It limits the possibility of anonymous movement and anonymous use of services, and more generally the possibility to remain unnoticed. Protection of public space for the exercise of fundamental rights and freedoms, in particular the right to freedom of expression, is crucial. If deployed extensively, for example on surveillance videos or police worn cameras, facial recognition technology can significantly redefine the nature of public space;[125] its use will not pass the test of necessity and proportionality. Indiscriminate and untargeted use of facial recognition which leads to mass surveillance in public spaces should never be allowed.[126]

- **Right to protest**: Using facial recognition technologies during protests may discourage people from taking part in protests, having clear negative implications vis-à-vis the effective functioning of participatory democracy.[127] Even if applied to police violence in protests, facial recognition may still affect those protesters who do not engage in violence or bystanders. In other words, the deployment of facial recognition may generate a chilling effect whereby individuals alter their behaviour and refrain from exercising their rights to protest. People might thus be discouraged from meeting individuals or organisations, attending meetings, or taking part in certain demonstrations. Likewise, live facial recognition in public spaces can be used to target journalists, posing a chilling effect on individuals and societies access to information on protests.

- **Religious freedom**: The use of face recognition technologies could interfere with people's religious freedom.[128] This can happen, for example, if people are obliged to uncover their faces in public spaces contrary to their religious traditions, and if they are subject to fines or other negative consequences in case they do not.

Emotion recognition

Purposes and usage of emotion recognition technologies

Emotion recognition technology purports to infer an individual's inner affective state based on traits such as facial muscle movements, vocal tone, body movements, and other biometric signals. The technology is designed to use machine learning to analyse facial expressions and other biometric data and subsequently infer a person's emotional state. The private sector is deploying these technologies to target their advertising, attract customers' attention and influence their choices, among other purposes. They also appear extremely attractive for governments and law enforcement agencies who aspire to anticipate criminal activities, wipe out terrorist threats and police both public and private spaces.[129]

Much like other biometric technologies, the use of emotion recognition involves the mass collection of sensitive personal data in invisible and unaccountable ways, enabling tracking, monitoring, categorising, scoring, or profiling of individuals, often in real time. They are used in various settings, by border patrol or police officers, to visually identify "suspicious behaviours" or "terrorists."[130] Both States and private companies test and deploy emotion recognition technologies in way that have far reaching consequences, often in collaboration with each other.[131]

Effectiveness of emotion recognition technologies

There are two fundamental assumptions undergirding emotion recognition technologies: the first, that it is possible to gauge a person's inner emotions from their external expressions, and secondly, that such inner emotions are both discrete and uniformly expressed across the world. This idea, known as Basic Emotion Theory (BET), suggests that humans across cultures could reliably discern emotional states from facial expressions, which were claimed to be universal.[132] BET has been wildly influential, even inspiring popular television shows and films.[133] However, scientists have investigated, contested and largely rejected the validity of these claims and discredited the claim of universality of emotion expression through the years.[134]

Emotion recognition technologies to identify, monitor, track, and classify individuals across a variety of sectors are thus fundamentally problematic not because they work, but rather because the stakeholders who build and use these technologies *claim* that they work.[135] Even so, academic studies and real-world applications continue to be built on the basic assumptions about universality of emotional expression, despite being rooted in dubious scientific studies and a history of discredited and racist pseudoscience.[136]

Challenges raised by emotion recognition technologies to human rights

Many concerns about the deployment and usage of emotion recognition technologies are similar to those mentioned above for biometric technologies and for facial recognition. These technologies are also being developed and deployed in invisible, opaque and unfettered manner with no oversight mechanisms or public consultations. Additionally, we highlight the following concerns:

- Emotion recognition technologies are based on **flawed pseudoscientific foundations and long discredited scientific assumptions**. As noted earlier, it is based on assumptions that expressions are universal, that emotional states can be unearthed from facial expressions, and that such inferences are reliable enough to be used to make decisions. All three assumptions have been discredited by scientists across the world for decades, but this does not seem to hinder the experimentation and sale of these technologies. Although there are growing technical concerns about emotion recognition technologies from private developers, most of these critiques address the technical concerns of the surveillance industry at the expense of the human rights implications for those being monitored/spied upon or false positives.[137]

Challenges raised by the use of emotion recognition technologies to people's ability to exercise their freedom of expression

The use of emotion recognition technologies present similar challenges as facial recognition. The design and use of emotion recognition adds a layer of complication and arbitrariness to an already worrying trend, given the lack of a legal basis, the absence of safeguards, and the extremely intrusive nature of these technologies.

By claiming to infer people's "true" inner states and making decisions based on these inferences, the deployment of emotion recognition technologies cements **arbitrary** and **unilateral** assumptions about individuals as ground truth. This has two significant implications. First, it gives way for significant chilling effects on individuals' ability to exercise their right to freedom of expression. This is because the notion of not only being seen and identified, but also **judged** and **classified** functions as an intimidation mechanism to make individuals conform to "good" forms of self-expression lest they be classified as "suspicious," or "risky" depending on the used case. Second, given the wide range of current applications, it can normalise mass surveillance as a part of an individual's daily life, particularly in civic spaces. Importantly, freedom of expression includes the right not to speak or express oneself.[138]

The nature of these technologies is also at odds with the notion of preserving human dignity and constitutes a wholly unnecessary method of achieving the allegedly purported aims of national security, public order and other aims as the case may be. While international human rights standards carve out national security and public order as legitimate justifications for the restriction of human rights including restrictions on freedom of expression and privacy, these justifications do not give States free rein to arbitrarily procure and use technologies that prevent people from exercising their human rights, nor does it permit States to violate rights without providing narrowly tailored justifications and valid, specific reasons for doing so.

There is also a staggering **lack of transparency** from States and companies in context of the design, development, and deployment of emotion recognition technologies. While the impetus for developing applications is provided to both start-ups and well-established technology companies, justification from authorities for buying and encouraging these products, information about oversight mechanisms, safeguards during pilots, and data protection considerations are scarcely available in the public domain, if at all. Given the multiple ways in which emotion recognition technologies threaten human rights, States that use and purchase them are under the obligation to ensure adequate accountability, legal certainty, and procedural and legal transparency about their procurement and deployment.[139] Companies are also subject to transparency obligations under the Guiding Principles on Business and Human Rights, which requires business enterprises to have processes in place that enable the remediation of any adverse human rights impacts they cause or to which they contribute.[140]

ARTICLE 19's recommendations

Based on the foregoing, ARTICLE 19 suggests that stakeholders should adopt a human rights-based approach to the design, development and use of biometric technologies and comply with the following recommendations.

Importantly, until these recommendations are in place there should be a moratorium for development and deployment of all these technologies by both States and private actors.

Recommendation 1: Biometric mass surveillance should be banned

States should ban the use of biometric technologies for the indiscriminate and untargeted processing of biometric data in public and publicly-accessible spaces, both offline and online. States should also cease all funding for biometric processing programmes and systems that could contribute to mass surveillance in public spaces.

Recommendation 2: Design, development and use of emotion recognition technologies should be banned

By design, emotion recognition technologies are fundamentally flawed and are based on discriminatory methods that researchers within the fields of affective computing and psychology contest. They can never meet the narrowly defined tests of necessity, proportionality, legality, and legitimacy. Hence, their development, sale, transfer, and use should be banned.

States should also establish international norms that ban the conception, design, development, deployment, sale, export, and import of these technologies in recognition of their fundamental inconsistency with human rights.

Recommendation 3: The design, development and use of biometric technologies should respect the principles of legitimacy, proportionality, and necessity

Both States and private actors should perform an adequate case by case assessment of the legitimacy of the use of biometric technologies for a certain purpose. The simple availability of a technology must never become a sufficient reason for its deployment and use. The design, development and deployment of these technologies should be restricted to lawful purposes that are consistent with human rights standards and that do not undermine human dignity.

For invasive technologies such as **facial recognition**, the starting point for the assessment is to recognise that because of this intrinsic invasiveness the technology is

never harmless. For this reason, States should consider the ban on deployment of facial recognition as the norm, and the possibility to use it as an exception, which has to be justified and tied to a specific purpose.

When a legitimate purpose for the use of biometrics is identified, its development and deployment must meet a narrowly constructed test of necessity and proportionality: the technology has to be absolutely necessary to achieve the scope and there should be no other less invasive means to do so.

States should avoid the widespread use of biometric technologies, and especially, of facial recognition, in public spaces. The use of these technologies in public spaces limits the ability of individuals to express themselves and to participate to social life. It is of utmost importance that States resist the normalisation of surveillance, preserve the role of public space for democracy, and therefore guarantee individuals' rights to remain anonymous, protest and express themselves in such space.

States should ensure that neither they nor private actors ever use biometric technologies to target those individuals or groups that play significant roles in promoting democratic values, for instance journalists and activists.

Recommendation 4: States should set an adequate legislative framework for the design, development and use of biometric technologies

For the legitimate uses that meet the necessity and proportionality test, States should shape an adequate **legislative framework** for the development and deployment of biometric technologies, which should include, at minimum:

- Rules on collection, storage, and retention that adequately protect individuals' biometric data and provide sufficient guarantees against security breaches
- Requirements concerning the quality of data used for training the technologies; the mandatory implementation of internal audits, tests for accuracy and racial bias
- The obligation to perform ex ante data protection impact assessments and human rights impact assessments, subject to continual review
- The obligation, for developers and users alike, to prevent and minimise risks. This obligation should be tailored according to the level of risks identified
- Binding code of practice for the use by law enforcement agencies
- Specific provisions to avoid dual use or 'mission creep' in the use of biometric technology by public as well as by private actors.

Moreover, States should keep red lines as part of their regulatory toolbox with regards to biometrics.

Recommendation 5: The design, development and use of biometric technologies should be subject to transparent, open and public debate

As the use of biometric technologies increasingly target multiple critical societal processes and democratic values, their design, deployment and development should only be allowed following a public and open debate. It is essential that civil society coalitions and networks of experts are given proper voice in the debate. This will prevent individuals' rights and freedoms from succumbing to the economic interests of any industry and also prevent governments from using vaguely shaped and over broad security concerns to normalise mass surveillance.

Recommendation 6: Transparency requirements for the sector should be imposed and thoroughly implemented

States should publicly disclose all existing and planned activities and deployments of biometric technologies. There should also be a specific obligation to provide for public consultations on issues such as the human rights implications of the purchases of these technologies and whether the technologies at issue will be effective at achieving their intended purposes.

States should ensure the highest level of transparency and public oversight on public procurement processes for the acquisition, development, and deployment of biometric technologies. The transparency should include the criteria for bid assessments, the terms of public-private partnerships, the content of public contracts, and regular public reporting on approvals, purchase, and use.

States should ensure the right of access to information related to the design, development, and deployment of biometric technologies according to international standards. States should consider information about biometric technologies as “public information" under the scope of right to information laws and publish such information proactively as well as releasing such information through access to information requests.

States and private actors should regularly publish their data protection impact assessments, human rights impact assessments and risk assessment reports, together with a description of the measures taken to mitigate risks and protect individuals' human rights. The publication should not represent a ticking box exercise; it should rather be done in a manner that allows and facilitates feedback, dialogue, as well as push backs.

Recommendation 7: Accountability and access to remedies should be guaranteed

Legislative frameworks for the development and deployment of biometric technologies should provide for clear accountability structures and independent oversight measures. States should condition private sector participation in the biometric technologies used for surveillance purposes – from research and development to marketing, sale, transfer and maintenance – on human rights due diligence and a track record of compliance with human rights norms.

The legislative framework should also ensure access to effective remedies for individuals' whose rights are violated by the use of biometric technologies.

Recommendation 8: Private sector should design, develop, and deploy biometric systems in accordance with human rights standards

Companies engaged in the design, development, sale, deployment, and implementation of biometric technologies should:

- Ensure the **protection and respect of human rights** standards. In order to do so, they should adopt a human-centric approach and perform human rights impact assessment ex-ante
- Set adequate and **ongoing risks assessment** procedures in order to identify risks for the rights and freedoms of individuals, and in particular, their right to privacy and freedom of expression, arising from the use of biometric technologies. They should also adopt a risk minimisation approach.
- Provide **effective remedies** in case of violation of individuals' human rights.

Endnotes

1 See e.g. the Council of Europe, Directorate General Human Rights and the Rule of Law, Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data, January 2014, p. 44. SGBs also include face or remote iris recognition, anthropometrics (measurement of body morphology), or physiometrics (measurement of bodily functions, e.g. heart rate, blood pressure, and other physical states).

2 See e.g. S. Hood, Biometric Marketing: What Is Biometric Technology and How Can Marketers Use It?, Hitsearch, 15 October 2018.

3 C.f. e.g. Supreme Court of Illinois, Rosenbach v. Six Flags Entertainment Corporation, 2019 IL 123186.

4 See e.g. Panel of experts at the request of the European Commission, Ethics and data protection, 14 November 2018.

5 See e.g. European Data Protection Supervisor, Opinion 4/2015, Towards a new digital ethics, data dignity and technology, 11 September 2015.

6 See e.g. Centre for Data and Ethics and Innovation, Interim report: Review into bias in algorithmic decision-making, July 2019.

7 C.f. for example, the UN High Commissioner for Human Rights, Practical recommendations for the creation and maintenance of a safe and enabling environment for civil society, based on good practices and lessons learned, A/HRC/32/20, 11 April 2016.

8 In China, for example, the State is using an app to control people's access to public spaces, sending people's data to the police, see New York Times, In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, 1 March 2020. In the UK, the Government was planning to add facial recognition functionalities on the app sponsored by the NHS for contact tracing and also announced that this facial recognition could be the basis for the issuing of immunity passports, see e.g. The Telegraph, NHS app adds face-scanning sign ups in step towards immunity certificates, 19 May 2020. In Liechtenstein, part of the population now wears electronic bracelets that monitor skin temperature, breathing pulse and other biometrics. The Government plans to roll out the bracelet scheme for the entire country by autumn, see e.g. L. Cendrowicz, Coronavirus Testing: Liechtenstein tracks virus with pioneering biometric bracelets, iNews.co.uk, 16 April 2020.

9 See e.g. New Statesman, Facial verification tech in NHS app could pave way for immunity passports, 20 May 2020.

10 Currently, the use of these surveillance helmets is confirmed in China, Dubai and Italy; see e.g. Business Insider, Police in China, Dubai, and Italy are using these surveillance helmets to scan people for COVID-19 fever as they walk past and it may be our future normal, 17 May 2020.

11 For further discussion of this topic, see e.g. V. Marda, Papering over the crack: on privacy versus health, in Data Justice and Covid-19: Global Perspectives, 2020.

12 See e.g. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive), Article 3 (13); Regulation (EU) 2016/679 of

the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), Article 4(14); Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, Article 3(18).

13 See e.g. Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies.

14 See e.g. D. Hambling, The Pentagon has a laser that can identify people from a distance-by their heartbeat, MIT Technology Review, 27 June 2019.

15 See e.g. E. **Mordini & D. Tzovaras** (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context, Springer Netherlands, 2019.

16 See e.g. Article 29 Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, Brussels, 22 March 2012, p. 2.

17 ARTICLE 19, Emotional Entanglement: Freedom of Expression Implications of China's Emotion Recognition Market, 2020.

18 See e.g. Association for Psychological Science, Corrigendum: Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, 2016; or L. Feldman Barrett et al., Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest. Volume 20, Issue 1, 2019.

19 See e.g. A. Korte, Facial recognition technology cannot read emotions, scientists say, American Association for the Advancement of Science, 16 February 2020; or S. Porter, Secrets and Lies: Involuntary Leakage in Deceptive Facial Expressions as a Function of Emotional Intensity, Journal of Nonverbal Behavior, 36(1):23-37, March 2012.

20See e.g. A. M'charek, Tentacular Faces: Race and the Return of the Phenotype in Forensic Identification, American Anthropologist, 6 May 2020.

21 See e.g. R. Wevers, Unmasking biometrics' biases: Facing gender, race, class and ability in biometric data collection, Tijdschrift voor Mediageschiedenis 21.2 (2018): 89-105, TMG Journal for Media History.

22 For an overview, see e.g. S. Fussel, An Algorithm That 'Predicts' Criminality Based on a Face Sparks a Furor, Wired, 24 June 2020; K. Amjad & A.A. Malik, A Technique and Architectural Design for Criminal Detection based on Lombroso Theory Using Deep Learning, LGURJCSIT Vol. 4 No 3 (2020).

23 See e.g. INTERPOL, Biometrics for Frontline Policing; or The Brussels Times, The Brussels Airport to be equipped with facial recognition cameras, 9 July 2019.

24 See e.g. the Aadhaar program in India, the South Africa national ID card system, PYMNTs; or Deep Dive: Digital ID Developments From Around The World, 27 February 2019.

25 C.f. Metropolitan Police and NPL, Metropolitan Police Service Live Facial Recognition Trials, February 2020.

26 See e.g., V. Marda & S. Narayan, Data in New Delhi's predictive policing system, 2020; or A. Daly, Algorithmic oppression with Chinese characteristics: AI against Xinjiang's Uyghurs**, 2019.**

27 The increasing deployment of biometrics by the State to deliver public services, together with the risks of this approach, have been flagged by the UN Special Rapporteur on

extreme poverty and human rights in her 2019 Report to the General Assembly, see UN Special Rapporteur on extreme poverty, Digital Technology, social protection and human rights, A/74/493, October 2019.

28 See e.g. Thales biometric systems in electoral rolls; according to their website, the countries include the Democratic Republic of Congo, Gabon, Oman, Burkina Faso, Benin, the Philippines and Sweden.

29 C.f. e.g. Supreme Court of Illinois, Rosenbach v.Six Flags Entertainment Corporation, 2019 IL 123186.

30 Similar remarks are made by UN Special Rapporteur on extreme poverty, op.cit.

31 Through its adoption in a resolution of the UN General Assembly, the UDHR is not strictly binding on states. However, many of its provisions are regarded as having acquired legal force as customary international law since its adoption in 1948; see Filartiga v. Pena-Irala, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).

32 UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, UN Treaty Series, vol. 999, p. 171.

33 Article 10 of the European Convention on Human Rights (European Convention), 4 September 1950; Article 9 of the African Charter on Human and Peoples' Rights (Banjul Charter, African Charter), 27 June 1981; Article 13 of the American Convention on Human Rights (American Convention), 22 November 1969; and Article 11 of the EU Charter on Fundamental Rights (EU Charter).

34 HR Committee, Belichkin v. Belarus, Comm. No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

35 HR Committee, General Comment No. 34, Article 19: Freedom of Opinion and Expression, CCPR/C/GC/34, para 18.

36 Ibid., para 19. The same language is repeated in regional human rights conventions, most notably Article 13 of the American Convention, Article 9 of the African Charter, Article 10 of the European Convention, and Article 23 of the ASEAN Human Rights Declaration.

37 IntConvention on the Elimination of All Forms of Racial Discrimination, 21 December 1965, UN Treaty Series, vol. 660, p. 195.

38 Article 11 of the European Convention, Article 12 of the EU Charter, Article 15 of the American Convention and Article 11 of the African Charter.

39 HR Committee, General Comment No. 37, Article 21: right of peaceful assembly, CCPR/C/GC/37, 27 July 2020, para 36.

40 Article 11 of the American Convention; and Article 8 of the European Convention.

41 C.f. the HR Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, para 3; International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles), Principle 1.

42 European Convention, op. cit., Article 14; EU Charter, op. cit., Article 21; African Charter, op. cit., Articles 2 and 3; American Convention, op. cit., Article 24.

43 ICCPR, Article 26.

44 C.f. e.g. ARTICLE 19, The Global Principles on Protection of Freedom of Expression and Privacy, 2017.

45 General Comment No. 16, op.cit., para 10.

46 Guidelines for the Regulation of Computerized Personal Data Files, GA Res. 45/95, 14 December 1990.

47 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108.

48 Under Article 1 of the EU Charter, human dignity is the foundation of all fundamental rights guaranteed therein. Therefore, biometric data must be collected and processed in a manner that adequately protects human dignity; c.f. also CJEU, C-377/98, Netherlands v. European Parliament and Council, 9 October 2001, paras. 70-77. Additionally, pursuant to Article 52 (1) of the EU Charter, any limitation on fundamental rights must: (i) be provided for by law. This requirement calls for an appropriate legal basis meeting qualitative requirement: the rule has to be public, precise and foreseeable; (ii) genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; (iii) respect the essence of the right; (iv) be necessary and proportionate. The European Data Protection Supervisor (EDPS) provides stringent guidance about demonstrating necessity and proportionality. The Fundamental Rights Agency (FRA) considers that the use of facial recognition can violate human dignity by making people avoid important places or events; through excessively forceful/coercive ways that data might be collected; and through "inappropriate police behaviour;" see e.g. FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement, Vienna, 2020, p. 20.

49 African Union Convention on Cyber Security and Personal Data Protection, 2014. ARTICLE 19 notes that in our view the criminal penalties and content-based regulations present in the Convention fall short of the standards of permissible limitations on freedom of expression under other binding human rights instruments.

50 OAS, Principles for Privacy and Personal Data Protection in the Americas, 2015, currently under revision. Revisions include specific references to biometric data.

51 HR Committee, General Comment No. 16 (Article 17 ICCPR), 8 April 1988, para 10; in which the HR Committee noted that the right is necessary in order to ensure respect of the right to privacy.

52 Ibid.

53 C.f. European Court, Gaskin v. the United Kingdom, 7 July 1989, Series A no. 160, para 49; M.G. v. the United Kingdom, App. No. 39393/98, 24 September 2002, para 27; Odièvre v. France [GC], App. No. 42326/98, ECHR 2003III), paras 41-47; Guerra and Others v. Italy, App. No. 14967/89, 19 February 1998.

54 GDPR, op.cit.

55 FRA, Opinions Biometrics, 2019.

56 See e.g. the Illinois State Biometric Information Privacy Act, which recognised that "an overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information;" Illinois Compiled Statutes 740 ILCS 14/1 Biometric Information Privacy Act, Sec 5 (d).

57 Special Rapporteur on freedom of expression, Report on encryption, anonymity, and the human rights framework, A/HRC/29/32, 22 May 2015.

58 HRC, Resolution on the Right to Privacy in the Digital Age, UN Doc. A/HRC/RES/34/7, 23 March 2017, para 2.

59 Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108.

60 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 9.

61 Ibero-American Data Protection Network (RIPD), Data Protection Standards of the Ibero-American States, Articles 2.1(d) and 29.4.

62 African Union Convention on Cyber Security and Personal Data Protection, cit. Article 10.4(d).

63 UN High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/39/29, 3 August 2018, para 14.

64 Ibid., para 61 c).

65 Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, A/HRC/41/41 17 May 2019, para 57.

66 Biometric Update, Biometric Update, UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition, 3 July 2018.

67 OHCHR, UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools, 25 June 2019.

68 European Court, S. and Marper v. the UK [GC], App. Nos. 30562/04 and 30566/04, 4 December 2008, paras 112 and 125.

69 UN Security Council, Resolution 2396 (2017).

70 2018 Addendum to the 2015 Madrid Guiding Principles, Annex to the letter dated 28 December 2018 from the Chair of the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism addressed to the President of the Security Council.

71 UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, Compiled by CTED and UNOC, 18 June 2018.

72 Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (The Ruggie Principles), A/HRC/17/31, 21 March 2011, Annex. The UN Human Rights Council endorsed the guiding principles in HRC resolution 17/4, A/HRC/RES/17/14, 16 June 2011.

73 Guiding Principles on Business and Human Rights: Implementing the UN 'Protect, Respect and Remedy' Framework, developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie, 7 April 2008, A/HRC/8/5A/HRC/17/31. The Human Rights Council endorsed the Guiding Principles in its resolution 17/4 of 16 June 2011.

74 Ibid., Principle 15.

75 Some companies have gone even further than that and started to develop their own guidance lobbying legislators to enact them; see e.g. Vox, Jeff Bezos says Amazon is writing its own facial recognition laws to pitch to lawmakers, 26 September 2019.

76 Special Rapporteur on FoE, Report to the Human Rights Council on Freedom of expression, states and the private sector in the digital age, 2013, A/HRC/32/38, 11 May 2016.

77 Google, Artificial Intelligence at Google: Our Principles.

78 An EU-wide asylum fingerprint database, the European Asylum Dactyloscopy Database (EURODAC) is meant to store fingerprints of all people who cross a European border. However, concerns were raised, when it was announced that the information in the database would be made available to law enforcement authorities and Europol in their terrorism investigations. The repurposing of the database for terrorism purposes rather than for immigration further stereotypes and stigmatises an already

vulnerable population: asylum seekers, who are already fleeing persecution, are being immediately associated with terrorist acts; see Statewatch and PICUM, Data protection, Immigration Enforcement and fundamental Rights: What's the EU's Regulations on Interoperability Mean for People with Irregular Status.

79 S. and Marper v. the UK, op.cit., para 103.

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

81 CNIL, Facial Recognition: For the debate of the issues at stake (in French), 15 November 2019, p. 6.

82 Ada Lovelace Institute and DataKind UK, Examining the Black Box: Tools for Assessing Algorithmic Systems, 29 April 2020.

83 For example, the UK company Sthaler developed a biometric system for customer authentication and security to be used at music festivals. The system is currently being deployed for other purposes too; see, e.g. From Sthaler to FinGo.

84 German Data Ethics Commission, Opinion, October 2019.

85 The Administrative Tribunal of Marseille, 27 February 2020, req. n. 1901249.

86 Where accompanied by appropriate legal and procedural safeguards, targeted interception of an individual's communications is a legitimate act of a democratic government, which can be necessary to prevent crime and disorder and protect national security. Targeted surveillance may only be justified when it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued; See, e.g. European Court, Klass and others v. Germany, App. No. 5029/71, 6 September 1978. The European Court has used the concept of "reasonable expectation of privacy" – the extent to which people can expect privacy in public spaces without being subjected to surveillance – as one of the factors, to decide whether there is a violation of the right to respect for private life under the European Convention; see European Court, Copland vs the UK, App. Nos. 62617/00, 3 July 2007, para 42. In a similar vein, the European Data Protection Board (EDPM), in its guidelines on processing personal data through video devices, states that individuals "can also expect to be free of monitoring within publicly accessible areas especially if those areas are typically used for recovery, regeneration, and leisure activities as well as in places where individuals stay and/or communicate, such as sitting areas, tables in restaurants, parks, cinemas and fitness facilities. Here the interests or rights and freedoms of the data subject will often override the controller's legitimate interests;" see EDPB, Guidelines 3/2019 on processing personal data through video devices, Version 2.0, 29 January 2020.

87 See e.g. P. Fussey & D. Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre, July 2019, p. 36 and fn. 87. See also, the International Justice and Public Safety Network, Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, 30 June 2011, Document p. 016632; which states that "the use of face recognition for surveillance purposes has the potential to make people feel extremely uncomfortable, cause people to alter their behaviour, and lead to self-censorship and inhibition." See also Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, A/HRC/44/24, p. 34.

88 C.f. European Court, Szabó and Vissy v

Hungary, App nos. 37138/14, 12 January 2016, para 38. See also Human Rights Watch & Pen International, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy, July 2014; and CNIL, 2019 report, op.cit. (the CNIL noted that constant surveillance and facial recognition in public spaces can make seemingly normal attitudes and behaviours appear suspect, such as wearing sunglasses, having one's hood up, or staring at the ground or a phone).

89 See e.g. FRA 2020 report, op.cit., p. 20; or London Policing Ethics Panel, Final Report on Live Facial Recognition, May 2019.

90 Surveillance and Human Rights, op. cit., p. 26.

91 See e.g. The Indian Express, Delhi Police film protests, run its images through face recognition software to screen crowd, 28 December 2019; India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP, 11 March 2020.

92 Surveillance and Human Rights, op.cit., p. 15.

93 See e.g. the Committee on Standards in Public Life, Artificial Intelligence and Public Standards, Section 4.7: Impact Assessment, February 2020. The Committee noted that proper accountability depends on public bodies being aware of the risks of their AI systems, so that authorities could be assessed against any mitigation measures they take.

94 In December 2020, the US Court of Appeals for the Ninth Circuit welcomed the applicant's arguments that access to information requests seeking access to aggregate data are essential to balance the public's interest in understanding how the government uses biometric and other personal data it collects without disclosing the underlying data that is often private or otherwise intrusive; see US Court of Appeals for the Ninth Circuit, The Center for Investigative Reporting v. United States Department of Justice, No.18-17356D.C. No. 3:17-cv-06557-JSC, 3 December 2020. See also See e.g. EPIC v. FBI- Next Generation Identification; and US Government Accountability Office, Face Recognition Technology Report and Recommendations, May 2016.

95 E.g. in the UK, the Office of the Commissioner for the Retention and Use of Biometric Material, whose role is to provide independent oversight of the regime established by the Protection of Freedoms Act 2012 and to govern the retention and use by the police in England and Wales of DNA samples, profiles and fingerprints, it is not covered by the Freedom of Information Act. Thus, the UK Office has no legal obligation to reply to access to information requests. For further information on the mandate and power of the Biometrics Commissioner see the Office of Biometrics Commissioner page on the UK Government's website.

96 Access to information requests have allowed individuals to obtain crucial information of facial recognition technology such as error rate, licence agreements between public bodies and private companies or dissemination of biometric data between agencies for a broad set of purposes; see e.g. EPIC's experience in the US in challenging the use of biometric technologies by various public agencies: EPIC FOIA: DHS Biometric Program. Access to information requests have also unveiled public agencies' failure to conduct a privacy audit of the agency's use of facial recognition or adequately test the accuracy of the technology; see, e.g. U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI should better ensure privacy and accuracy, 2016.

97 C.f. the UK Biometrics and Forensics Ethics Group Principles, December 2020.

98 Indeed, 1:1 verification systems raise challenges too; see, e.g. A. Kak, The State of Play and Open Questions for the Future,

Regulating Biometrics: Global Approaches and Urgent Questions, September 2020.

99 See e.g. FRA, 2020 report, op.cit.

100 See e.g. Planet Biometrics, Met begins operational use of Live Facial Recognition (LFR), 24 January 2020; EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade, 4 December 2019; Human Rights Watch, Facial Recognition Deal in Kyrgyzstan Poses Risks to Rights, 15 November 2019; or The Times of India, From protest to chai, facial recognition is creeping up on us, 5 January 2020; The Ken, Watch this space: New Bill could unleash facial recognition free for all, 11 February 2020.

101 For example, in Brazil, facial recognition systems have been applied since at least 2011, and their use for security purposes has been broadly expanded in 2019, mainly during Carnival, through partnerships with private agents. Today, more than 40 cities in the country have adopted the technology. See e.g. Le Monde Diplomatique Brasil, Facial recognition: the trivialization of controversial technology (in Portuguese), 22 April 2020. For an overview of the use of face recognition technologies in Brazil, see Instituto Igarape, Infografic of Facial Recognition in Brazil (in Portuguese).

102 See e.g. The Guardian, Facial recognition… coming to a supermarket near you, 4 August 2019; Big Brother Watch, Co-op Facial Recognition Supermarkets Revealed, 14 January 2021.

103 See e.g. Brazilian Institute of Consumer Protection (Instituto Brasileiro de Defensa do Consumidor, IDEC), IDEC wants to know how Hering uses facial recognition data from customers (in Portuguese), 6 March 2019.

104 See e.g. IDEC, IDEC asks for clarification on facial data collection in Carefour store (in Portuguese), 23 April 2019.

105 See e.g. IDEC, Justice prevents use of camera that collects facial data in subway in SP (in Portuguese), 18 September 2018.

106 See e.g. The Telegraph, Uber faces racism claim over facial recognition software, 23 April 2019.

107 For example, Huawei puts facial recognition at the heart of its 'Safe City' project, which the company is trying to develop in many cities all around the world, with particular focus on African and Asian regions; see e.g. CSIS, Watching Huawei's "Safe Cities," 4 November 2019.

108 For example, in 2019, San Francisco banned the use of facial recognition by law enforcement agencies; see e.g. EFF, Stop Secret Surveillance Ordinance (05/06/2019) (for the banning order) and The Guardian, San Francisco was right to ban facial recognition. Surveillance is a real danger, 30 May 2019. Portland is currently discussing a ban that encompasses the use by both public and private actors; see, e.g. Fast Company, Portland plans to propose the strictest facial recognition ban in the country, 12 February, 2019. In the UK, Police Scotland revealed that they would not yet be deploying facial recognition technology as it was "not fit for use" due to, among others, human rights and privacy concerns. Plans for deployment, initially for 2026, have been put on hold in order for a wider consultation to be held on the impact of the software; see, e.g. BBC, Facial recognition: 'No justification' for Police Scotland to use technology, 11 February 2020.

109 For example, IBM, in a letter to the US Congress on Racial Justice Reform, announced it would stop the sale of 'general purpose' face recognition software; see IBM CEO's Letter to Congress on Racial Justice Reform, 8 June 2020. Amazon announced a one-year moratorium on police use of its Rekognition technology, see Amazon, We are implementing a one-year moratorium on police use of Rekognition, 10 June 2020. Microsoft vowed not sell to law enforcement agencies its face recognition technologies;

see, e.g. The Washington Post, Microsoft won't sell police its facial recognition technology, following similar moves from Amazon and IBM, 11 June 2020.

110 See, e.g. New York Times, The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?, 28 March 2019.

111 For example, in Moscow, the administration is using facial recognition technology to ensure people ordered to remain at home or at their hotels under coronavirus quarantine; see, e.g. Reuters, Moscow deploys facial recognition technology for coronavirus quarantine, 21 February 2020. Chinese companies are rolling out FR technology that can detect elevated temperatures in a crowd or flag citizens not wearing a face mask; see e.g. The Guardian, 'The New Normal': China's excessive coronavirus public monitoring could be here to stay, 9 March 2020. The UK is considering FR as instrumental to the establishment of an immunity passport system.

112 See e.g., Facewatch, Facewatch launces facemask recognition upgrade, 11 May 2020.

113 Worryingly, the European Commission seems to endorse this approach, and has recently awarded its 'seal of excellence' to the Aware technology, developed by the Spanish-based Herta Security, which provides advanced video analytics, including real-time face recognition and crowd behaviour analysis, to be used in the bloc's fight against another potential outbreak of the coronavirus. See e.g. Euractiv, Crowd monitoring facial recognition tech awarded seal of excellence, 19 June 2020.

114 In early 2019, the Serbia Minister of Interior and the Director of Police announced the placement of 1000 cameras on 800 locations in Belgrade. The public was informed that these surveillance cameras will have facial and license plate recognition software. Three civil society organisations in the country published a detailed analysis of the Ministry of Interior's DPIA on the use of smart video surveillance, which concluded that it did not meet the formal or material conditions required by the Law on Personal Data Protection in Serbia. The Serbian data protection authority confirmed the findings. For more information, see, e.g. EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade, 4 December 2019.

115 On February 2020, Facebook settled a class action in Illinois where users claimed that the company site's photo-tagging system used facial recognition technology to analyse their photos and create and store 'face templates' without informing users nor asking for their consent as of June 2011; see, e.g. New York Times Facebook to Pay $550 Million to Settle Face Recognition Suit, 29 January 2020. Similarly, Clearview AI app for facial recognition was developed and widely marketed to law enforcement agencies based on a database of 3 billion images illegally scraped from Facebook, Google and YouTube. The company is currently facing a lawsuit filed on behalf of several Illinois citizens for violation of the state's Biometric Information Act. In March 2020, Vermont Attorney General filed a lawsuit against the company defining its business practices as 'unscrupulous, unethical and contrary to public policy;' see e.g. Gizmodo, We Found Clearview AI's Shady Face Recognition App, 27 February 2020; or Vermont Attorney General Office, Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law, 10 March 2020.

116 See e.g. OneZero, Why you can't really consent to Facebook's Facial Recognition, 30 September 2019; E. Selinger & W. Hartzog, The Inconsentability of Face Surveillance, 66 Loyola Law Review 101 (2019).

117 See e.g. the National Institute of Standards and Technology, NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, 19 December 2019; D. Leslie,

Understanding bias in facial recognition technologies, The Alan Turing Institute, 2020; A. Najibi, Racial Discrimination in Face Recognition, 24 October 2020.

118 See e.g. J. Buolamwini & T. Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 2018. Also, the National Institute for Standards and Technology (NIST) recently performed a study to assess how accurately FR software tools identify people of varied sex, age and racial background. According to their findings, the answer depends on the algorithm at the heart of the system, the application that uses it and the data it is fed with. However, a NIST study found that the majority of face recognition algorithms exhibit demographic differentials. A differential means that an algorithm's ability to match two images of the same person varies from one demographic group to another. African American women resulted to be the demographic with the higher number of false positives; more in general, Asian, African American and native groups are the demographics that are most subject to inaccurate results; see NISTIT, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 8280.

119 See e.g. ACLU, Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, 26 July 2018 (which documented that the facial recognition system developed by Amazon wrongly recognised 28 members of the US Congress, out of 535 tested, has having committed crimes and among them a disproportionally high number was black); University of Essex, Human Rights Centre, Independent Report on the London Metropolitan Police Service's Trial of Live Recognition Technology, July 2019 (which found that app. 80% matches were wrong in six live trials by the UK Metropolitan Police in the London areas of Soho, Romford and Stratford); Stark, Face Recognition is the Plutonium of AI, 17 April 2019 (that warned that racial bias is a feature of FR technologies, rather than a bug).

120 Ibid. ACLU. Moreover, there are at least three reported cases of black men in the United States being wrongfully arrested because of faulty face recognition; see e.g. NBCNews, Man wrongfully arrested due to facial recognition software talks about 'humiliating' experience, 26 June 2020; The New York Times, Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match, 29 December 2020; The New York Times, Wrongfully Accused by an Algorithm, 24 June 2020.

121 C.f. e.g. Interpol, Facial Recognition.

122 See e.g. the UK Information Commissioner's Office, ICO investigation into how the police use facial recognition technology in public places, 31 October 2019.

123 See e.g. ARTICLE 19, Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence, April 2019; ARTICLE 19 and Privacy International, Privacy and freedom of expression in the age of artificial intelligence, April 2018.

124 In 2019, CNIL, the French data protection authority condemned the use of face recognition technology aimed to smooth and control children's access to school on the grounds that the same objective can be achieved by means which are less invasive of children's fundamental rights; see CNIL, op.cit. Several NGOs also denounced the implementation of this facial recognition technology in schools; see, e.g. La Quadrature du Net, the League of Human Rights, CGT Educ'Action des Alpes-Maritimes and the Federation of Parents' Councils of Public Schools in the Alpes-Maritimes, Facial Recognition in High Schools: A recourse to block biometric surveillance, 19 February 2019. See also Administrative Court of Marseille, 9th ch., Judgment of 27 February 2020. Incidentally, the French magistrate, involved in a relevant case in Marseille, stated during the hearing that "the Region is using a hammer to hit

an ant" which perfectly visualises the lack of proportionality between the measure implemented (FR system) and the objective to be achieved (controlling students' access). In a similar vein, students, from various schools across US cities, have protested against the use of facial recognition and in some cases, this has led to the school management abandoning the plan to deploy the technology. See e.g. The Guardian, Ban this technology': students protest US universities' use of facial recognition, 3 March 2020.

125 Civil society around the world started to raise its voice about the impact of FR surveillance on anonymity and about its chilling effect on freedom of expression. For example, in Australia, the deputy director of the New South Wales Council for Civil Liberties, in the context of the NSW parliamentary enquiry about the deployment of facial images matching systems said that "this brings with it a real threat to anonymity. But the more concerning dimension is the attendant chilling effect on freedoms of political discussion, the right to protest and the right to dissent. We think these potential implications should be of concern to us all;" see The Guardian, Facial image matching system risks 'chilling effect' on freedoms, rights groups say', 7 November 2018.

126 See e.g. E. Denham, Information Commissioner, Blog: Live facial recognition technology – police forces need to slow down and justify its use.

127 By way of example, the Home Ministry in India, on February 2020, arrested 1100 people who participated in peaceful protests, identifying them with the use of face recognition. See India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP, op. cit.

128 Religious freedom is guaranteed by Article 18 UDHR and given effect by the provisions of Article 18 ICCPR, as well as other regional and national instruments.

129 Ibid.

130 See e.g. US Transportation Security Authority's SPOT program or Europe's iBorderCtrl (a pre-screening AI system whose cameras scanned travellers' faces for signs of deception while they responded to border security agents' questions, trialled in Hungary, Latvia, and Greece). Critiques of the programs' dataset, false positives, and discriminatory potential led to its retraction. See e.g. Government Accountability Office, Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities, 14 November 2013; Department of Homeland Security Office of Inspector General, TSA's Screening of Passengers by Observation Techniques, May 2013; ACLU vs. TSA, 8 February 2017; Ars Technica, TSA's got 94 signs to ID terrorists, but they're unproven by science, 13 November 2013; The Intercept, Exclusive: TSA's Secret Behavior Checklist to Spot Terrorists, 27 March 2015; Ars Technica, The premature quest for AI-powered facial recognition to simplify screening, 2 June 2017; J. Sánchez-Monederoa & L. Dencik, The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl'; The Intercept, We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive, 26 July 2019.

131 For example, Chinese Alpha Hawkeye's emotion recognition system is used by authorities at Yiwu Railway Station to apprehend "criminals;" state-owned Chang'an Automobiles marketing cars with emotion and fatigue detectors; Hikvision is collaborating with Hangzhou Educational Technology Centre (which is in charge of edtech procurement for primary and secondary schools in the city), supervised by Hangzhou Education Bureau.

132 See e.g. P. Ekman, E. Richard Sorenson & W. V. Friesen, Pan-Cultural Elements in Facial Displays of Emotion, Science, 1969, Vol. 164, Issue 3875, pp. 86 – 88; P. Ekman, Universal Facial Expressions of Emotions, California Mental Health Research Digest,

8(4), 151-158, 1973; P. Ekman, Universals and Cultural Differences in Facial Expressions of Emotions, In Cole, J. (Ed.), Nebraska Symposium on Motivation (pp. 207-282), Lincoln, University of Nebraska Press, 1973.

133 See e.g. A. L. Hoffman & L. Stark, Hard Feelings - Inside Out, Silicon Valley, and Why Technologizing Emotion and Memory Is a Dangerous Idea, Los Angeles Review of Books, 11 September 2015.

134 See e.g. J. A. Russel, Is there universal recognition of emotion from facial expression? A review of the cross-cultural studies, Psychological Bulletin, 115(1), 102–141, 1994; L. Feldman Barrett et al, Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest, Vol. 20, Issue 1, 2019; Oxford Scholarship Online, Coherence between Emotions and Facial Expressions, The Science of Facial Expression, 2017; The New York Times, What Faces Can't Tell Us, 28 February 2014.

135 See e.g. A. Daub, The Return of the Face, Longreads, October 2018.

136 See e.g. L. Safra, C. Chevallier, J. Grezes & N. Baumard, Tracking historical changes in trustworthiness using machine learning analyses of facial cues in paintings, Nature Communications, 11, 4728, 2020; or Coalition for Critical Technology, Abolish the #TechToPrisonTimeline, Medium, 23 June 2020.

137 See e.g. C. Cun, C. Zhengdong & S. Beibei, Grasp the Truth in an Instant: Application of Micro-expressions Psychology in Customs Inspection of Passengers (in Chinese), Journal of Customs and Trade, 2018(03), pp. 31, 33.

138 C.f. General Comment 34, op.cit., which states that "any form of effort to coerce the holding or not holding of any opinion is prohibited. Freedom to express one's opinion necessarily includes freedom not to express one's opinion," para 10.

139 Report of the UN High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, 24 June 2020, para 40.

140 Guiding Principles on Business and Human Rights, op.cit., p. 15.

www.article19.org