EXECUTIVE SUMMARY

IMPACTS OF THE USE OF BIOMETRIC AND BEHAVIOURAL MASS SURVEILLANCE TECHNOLOGIES ON HUMAN RIGHTS AND THE RULE OF LAW

THE GREENS/EFA in the European Parliament

SECTION 2 INTRODUCTION

For centuries, citizens and residents have questioned the limits of the powers of the state to restrict their freedoms and free will. Each time these limits appeared to have been crossed in history, parliamentarians and civil society rose up. By the 18th century, this opposition was directed against passports and the registration of certain categories of persons in files, such as suspects of criminal offences and political opponents. By the end of the 19th century, public opinion opposed the collection, by the state, of their photographs, which was seen as a threat to the freedoms of *"honest people"*. People expressed fear of being subjected to arbitrary classification, based on opaque criteria, and to contestable deprivation of freedom on the sole ground of such categorisation.

From the First World War onwards, some governments succeeded in imposing identity documents on all their residents and then nationals, with a sorting process applying in certain countries to minorities that were regarded as undesirable. Identity cards survived the wars in France, Italy, and Germany, while they were abolished in the United Kingdom.

Opposition to events that had occurred during the wars led to the adoption, in 1950, of the European Convention on Human Rights (ECHR). The aim of the ECHR was and still is to prevent a return to totalitarianism, through a mechanism which discourages states from favouring order and security over the preservation of freedoms. Schematically, the ECHR requires as a minimum that any interference with a fundamental right be provided for by law, have a determined and legitimate purpose (which must correspond to a demonstrated need), and be both efficient and reduced to that which is strictly necessary to reach this purpose. These principles, also referred to as the *"requirements for necessity and proportionality"*, have been subject to specific implementation in laws dedicated to the protection of personal data from the 1970s onward, taking into account the ongoing digitisation of society.

From 1985 onward, developments of biometry and facial recognition, as well as the growing use thereof by public authorities and the private sector, have been feeding new concerns. Public authorities justify the implementation and further development of these technologies as a need that requires no discussion, in order to fight terrorism and ensure security. However, they have so far failed to establish any evidence of efficiency and added-value, whereas biometry is a highly intimate and identifying tool. Consequently, civil society and politicians alike are calling for an end to this culture of identification and control, which is widely considered a threat to democracy and the rule of law.

In this context, the current study aims to frame the terms of the debate in the most objective manner in order to identify whether human rights and the rule of law are under threat from the use of biometric and behavioural mass surveillance technologies, with a focus on the practices of public authorities. This evaluation is based on a privacy impact assessment (PIA) of biometric and behavioural mass surveillance technologies, understood as technologies that include the use of biometric identifiers and are likely to enable mass surveillance, even though they are not implemented for that particular purpose.

SECTION 3 CONTOURS AND CONTEXT OF THE USE OF SURVEILLANCE TECHNOLOGIES

The border management policies of the European Union (EU) successively imposed the implementation of biometrics in visas, passports, and identity cards. At the same time, the purpose of strengthening border management was extended to the preservation of the internal security of member states, to the prevention, detection and investigation of terrorist offences and other

serious criminal offences, and, in relation to specific databases, to cooperation in police and judicial matters. Nowadays, the information systems that support these policies, managed by eu-LISA, gather more than 53 million pieces of biometric data. These systems are the VIS, the SIS I and II, the Eurodac, the ECRIS, the ETIAS and the Entry/Exit System (EES). In addition, these systems use an Automated Fingerprint Identification System (AFIS), which is expected to include facial recognition as a major component in the future.

EU member states are also increasingly using video-surveillance, which progressively includes facial and behavioural recognition technology. In addition, the public and private sectors increasingly propose authentication functions based on biometric recognition. Both the private and the academic sectors also use surveillance techniques based on biometric or behavioural criteria.

The European Union plays a central role in the development of the use of biometric technology, seeking to favour a technical convergence of European systems that contain biometric data. This EU policy expands to the Western Balkans. This approach is sometimes presented as the result of pressure from the United States of America (USA) to make the recourse to biometry a priority objective in the fight against terrorism. However, authors show that actually the European Union made choices that widely exceeded the demands made by the USA and rather seem to serve an EU domestic policy aiming to develop a registry of fingerprints and facial images of EU citizens and residents..

The recording of biometric identifiers is implemented in a context where the EU and governments tend to short-circuit public debate and opposing opinions from parliamentarians and data protection authorities. At the same time, technological risks are often not seriously assessed, beyond rhetorical statements of commitment to fundamental rights protection. This observation raises the issue of the intentional weakening of parliaments and, more generally, of democratic checks and balances. In addition, we observe a high tendency, from the representatives of the EU and of members states, to force the *"acceptability"* of biometric identification and recognition through the kindling of *"an artificial atmosphere of fear"* (Guillaume Gormand), combined with a public communication which presents biometric surveillance in a favourable light. Indeed, it is shown as a pledge of security, the latter being asserted as a natural need that is beyond discussion in its principle, and which is inherent to freedoms or supersedes them. This approach tramples on fundamental principles that underpin the European legal system, in which security is conversely an exception to freedom, subject to strict conditions.

Citizens, deceived in relation to the efficiency and the purpose of biometric technology, are therefore deprived of any real debate on these topics. Yet, such a debate is of utmost importance. Indeed, security issues affecting intimate data that cannot be revoked and the question of whether the security brought by surveillance, including biometry, is real in the face of terrorist threat, are as important as the challenges at stake in terms of choice of social model, in relation to the one that is currently followed.

Regardless, the European Union sustains innovation by funding several research projects aiming at enhancing biometric or behavioural identification efficiency, such research having been criticised for not being ethical. This reproach is compounded by allegations of EU support for the implementation of surveillance technology in countries with poor human rights records, in the absence of any prior impact assessments.

In this context, a significant number of international organisations and institutions are calling for a ban on biometric surveillance, and particularly on facial recognition in publicly accessible places. They include the United Nations, the European Parliament, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS), as well as more than 170 non-governmental organisations (NGOs).

SECTION 4 THE LEGISLATION REGULATING SURVEILLANCE

1) ECHR AND EUCFR REQUIREMENTS

Historical excesses have shown the inability of states to ensure the protection of human rights in the absence of counter-powers, certainly because one of the main inherent characteristics of states is to give precedence to order over freedom. As a result, the European Convention on Human Rights (ECHR) was signed on 4 November 1950 in order to establish objective obligations for states towards individuals in relation to the protection of human rights, as well as establish a control mechanism of the enforcement of these rights (human rights being called *"fundamental rights"*, where they are protected by a European or international legal instrument). Nowadays, the ECHR is in force in the 47 member states of the Council of Europe, which include all the member states of the European Union.

It is of utmost importance to emphasise that respect for the dynamics of fundamental rights protection established in the ECHR is the vital condition for maintaining liberal democracy, understood as a form of government in which *"liberties are well protected and in which there exist autonomous spheres of civil society and private life, insulated from state control"* (Larry Diamond). Indeed, the design of such dynamics has been based on the works of great thinkers, such as Beccaria and Tocqueville, who looked at history with lucidity and warned about the dangers of coming out of a system in which governments are prevented from prioritising security over freedom. As a result, the legal system is designed in such a way so as not to pit freedom against security.

The dynamics of fundamental rights protection established in the ECHR is fourfold.

Firstly, limitations of freedoms must be provided for by a clear law that ensures foreseeability.

Secondly, limitations of freedoms must have a legitimate aim.

Thirdly, limitations of freedoms must be efficient in the pursuit of a legitimate purpose, determined within the broader sphere of the above-mentioned legitimate aim. This purpose must be connected with a need, for society, which itself must be demonstrated.

Fourthly, limitations of freedoms must be reduced to the strict minimum to reach this purpose. This implies both the minimisation of impacts on fundamental rights and the setting up of guarantees and safeguards such as transparency, foreseeability, and independent control.

The principles of legitimate and determined purpose on the one hand and of efficiency on the other hand together form the principle of *"necessity"*. The principle of strict minimum, implying minimisation and the setting-up of guarantees against arbitrariness, forms the principle of *"proportionality"*. In the current study, we analyse the principle of legal basis under the principle of proportionality, because it is one of its components, as it ensures foreseeability and a kind of *"constraining transparency"* for the person who is restricting the fundamental rights of other persons. We further analyse the principle of legitimate purpose as an element of the requirement for necessity, since, in the same line, it is also fundamentally one of its components.

Compliance with all these requirements must be subject to the supervision of a parliament with effective decision-making powers and of independent judges who can adjudicate cases brought by concerned individuals. Getting away from this path, all the terms of which are of utmost importance, implies taking a road which inexorably leads to totalitarianism. Remaining deaf to this alert can only induce a denial of history, as recalled by many eminent specialists, constitutional courts, and supreme courts.

These principles apply to all the rights and freedoms that are at stake where surveillance technologies are in use, unless the ECHR or the European Court of Human Rights (ECtHR) provide for more restrictive conditions. These rights are the right to

private and family life, the right to the protection of personal data, the right to freedom of expression, the right to freedom of assembly and association, the right to freedom of opinion, the right to freedom of movement, the right to liberty, the right to non-discrimination, the right to education, the right to a fair trial, the right to dignity and to self-determination, and the right to resist oppression.

2) EUROPEAN UNION LEGISLATION

At the level of the European Union, the EU Charter of Fundamental rights (EUCFR) offers the same protection as the ECHR, in terms of meaning and scope, to the rights it protects and that are also enshrined in the ECHR. Personal data protection is further clarified in the EU General Data Protection Regulation (GDPR), which applies to all kinds of personal data processing operations, to the exclusion of strictly personal activities and of judicial processing activities. Data processing activities by courts and police departments are regulated by the so-called *"Police-Justice"* Directive. However, the latter and the GDPR do not apply to the activities of units dealing with national security. That being said, the ECHR requirements remain applicable to such units.

Besides the legal instruments organising the protection of personal data, the European Union issued a series of successive legal instruments which impose on states the collection of biometric identifiers for the purpose of migration control. Subsequently, the list of the objectives of this legislation has been further extended.

In addition, on 21 April 2021, the European Commission issued a proposition aiming to lay down harmonised rules on artificial intelligence (AI). The proposed *"Artificial Intelligence Act"* frames the placing on the market, the putting into service, and the use of AI systems in the Union. At the same time, it differentiates between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk. In particular, the proposed regulation considers that 'real-time' and 'post' (or 'after recording') remote biometric identification systems should be classified as high-risk and that, as a result, they should be subject to specific requirements on logging capabilities and human oversight. The proposed regulation further prohibits as a principle the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement. However, this prohibition can be bypassed by national law within certain limits and under the reserve that a series of safeguards is implemented. In addition, the prohibition does not apply to *"post"* identification, neither to 'real-time' and *"post"* remote biometric identification that would be operated by the private sector or by public authorities for national security purposes.

SECTION 5 IMPACTS OF THE USE OF MASS SURVEILLANCE TECHNOLOGIES ON HUMAN RIGHTS

1) THE SOURCES OF IMPACTS FOR HUMAN RIGHTS

The sources of impacts on human rights are actions, behaviours, or initiatives which limit the exercise of these rights. For example, the simple fact of collecting biometric identifiers limits the right to personal data protection. Impacts on human rights must comply with the requirements established in the ECHR, in the EUCFR, and in other potential EU and national legislation that enforce thosse texts in specific areas, such as the GDPR. These requirements differ, depending on the human right at stake. Some fundamental rights are deemed to be absolute and do not suffer any limitation. One example is the case of the freedom to hold a belief. Some other fundamental rights are deemed conditional and can be limited subject to strict conditions, for example the case of the right to physical liberty. A final group of fundamental rights can be restricted following the general requirements for necessity and proportionality.

Impacts on fundamental rights that comply with the above-mentioned rules are deemed legitimate and, based on the ECHR, lawful. Impacts on fundamental rights that do not comply with these rules are deemed arbitrary, and they constitute a violation of the fundamental right that they restrict. They constitute a violation as such, even though the person whose rights are limited does not suffer, spiritually or physically, from this limitation. Indeed, these requirements not only protect individuals, but also democratic rules and the rule of law, by establishing that everyone respect the rights of others.

Illegal impacts are the ones that must be identified and prevented. The identification of such impacts takes place in two stages. The first stage consists of checking that known practices and legislation comply with the principles of limitation of fundamental rights. In the current study, we limit this analysis to compliance with the requirements for necessity and proportionality because they apply to the right to respect for private life, which is the primary fundamental right to be limited by the use of biometric technology. The right to respect for private life, in turn, offers protection of dignity, self-determination, and of a series of other rights such as the freedom of expression and the right to not be subjected to discrimination. The second stage consists of analysing risk to rights and freedoms, in order to ensure that all potential impacts, even indirect, have been identified.

2) ASSESSMENT OF THE COMPLIANCE OF THE USE OF MASS SURVEILLANCE TECHNOLOGIES WITH THE REQUIREMENT FOR NECESSITY AND PROPORTIONALITY

This assessment targets three pieces of primary or subordinate legislation, beyond biometric recognition practices: Regulation (EU) 2019/1157 which establishes the mandatory creation of biometric identity cards; the French Decree n° 2016-1460 which establishes a national database of biometric identifiers; and the proposed Artificial Intelligence Act of 21 April 2021. These three pieces of legislation failed the test of necessity and of proportionality.

Firstly, law and practices suffer from a lack of specification of purposes. In particular, the purposes that are put forward in legislation are far too broad and therefore do not respect the requirements for a determined, specific, and *"pressing"* purpose. In addition, several practices of diversion of purpose lead either to the extension of the scope of application of laws once they have been adopted, or to authorise the use, in any kind of penal proceedings, of evidence whose usage should be restricted to the defence of crucial purposes, such

as the fight against terrorism.

Secondly, the EU and member states failed to demonstrate the efficiency of the legal texts and practices under scrutiny, despite many requests to that effect. In particular, public authorities have thus far not demonstrated the extent to which the measures they propose are likely to assist in the fight against terrorism, crime and fraud.

Thirdly, laws and practices under scrutiny are disproportionate. Proportionality is difficult to assess where the purposes, efficiency, and added value of legislative provisions and practices are unknown. However, even without this information, it seems very tough to sustain that the proposed personal data processing operations do not go *"further than needed to fulfil the legitimate aim being pursued"*, to quote the Article 29 Data Protection Working Party. In particular, before these legislations, the management of national identity cards, the possibility to cross borders, and the fight against terrorism were all already effective. Conversely, the measures at stake concern the entire population, before any prohibited action has been attempted, based on the processing of personal data that is among the most sensitive type, along with DNA.

Fourthly, law and practices under scrutiny suffer from a lack of sufficient safeguards against arbitrariness.

The legal basis establishing restrictions of freedoms must comply with relevant national and international legislation. However, the EU legislations under scrutiny here are based on provisions of the Treaty on the Functioning of the European Union (TFEU) that actually cover neither the provisions imposing biometric identifiers in identity cards, nor the possibility to authorise member states to use facial recognition technologies in public areas.

In addition, adopting a law in compliance with democratic rules implies, in principle, that such law is discussed and adopted by a parliament with effective decision-making power. However, in some countries, the powers of parliament are undermined by several mechanisms which are often related to separation of powers. In addition, provisions that impact human rights for law enforcement or security purposes often disregard previous contrary opinions from parliamentary members and legitimate authorities such as data protection authorities and supreme courts, both at national levels and at the EU level. This is a worrying situation, because it means that governments and European institutions do not respect the counter-powers that have been established to ensure the proper democratic functioning of political systems. Worse, this means that parliaments often do accept to legislate according to the will of the government.

Parliamentary opposition, and more widely citizens' opposition, is further weakened by the form of communication which has been employed by public authorities for at least two decades. This communication promotes security at the top of freedoms, uses highly questionable assertions that stigmatise persons who oppose governmental views, and uses a vocabulary that presents interferences with rights as measures protective of these very rights.

These considerations are of utmost importance because democratic guarantees against arbitrariness can only be established by laws that are adopted with respect to democratic rules. Where the latter rules are disregarded, legal provisions adopted in that context cannot be assumed to be proportionate.

3) RISKS ON HUMAN RIGHTS

Risks for the right to private life firstly consist in a disproportionate loss of opacity for the individual. Indeed, a general and indiscriminate retention of biometric identifiers, as well as indiscriminate surveillance of publicly accessible places, before any offence has been committed, is, as such, a violation of the right to private life. The ECtHR stated many times that there must be a link between the conduct of the persons whose data is collected and the objective pursued by the legislation that provides for the collection of such data, in order for surveillance to be authorised. No argument can be put forward against this rule in a political democracy governed by the rule of law. Internal security is not a sufficient justification, as stated by the ECtHR.

Risks for the right to private life include unjustified loss of personal development and of personal autonomy. Indeed, individuals who feel they are being monitored may have a tendency to censor themselves, and therefore modify their behaviour or avoid meeting someone in a publicly accessible place. It is important to recall that this impact exists independently from the fact that the individuals concerned suffer, physically or psychologically, from it.

Risks for the right to private life also include a genuine, current, and serious threat to self-determination and to dignity, while both these rights suffer no limitation in a democracy governed by the rule of law. Data collected through visual and acoustical surveillance, as well as biometric characteristics that are used to identify or categorise people, relates to the human body and the human mind. Consequently, such data may inter alia disclose an important amount of information which is very intimate and which may further be biased. These categories of data particularly carry the risk, where processed, of amounting to *"a 'datafication' of humans"* (Christiane Wendehorst and Yannic Duller), which creates several possible impacts. A first impact is the risk of being treated with a lesser level of respect, compared to situations where decisions are made outside any personal data processing. Another possible impact, for the person concerned, is the risk of being subjected to an illegitimate decision, without any possibility of escape.

The main risk for the right to freedom of expression and the right to freedom of assembly is self-censorship, as shown by several specialists and legitimate authorities including the EDPB, the Council of Europe. and the German Supreme Court. It is worth recalling that freedom of expression is an *"essential foundation"* of democracy and the rule of law and *"one of the basic conditions for its progress"*, according to the ECtHR, and states have a positive obligation to ensure its effectiveness. This implies giving citizens the confidence that they can express themselves without fear, and therefore to not monitor them where not duly justified, necessary. and framed. This also implies, for public authorities, the obligation to not communicate in a way that stigmatises persons with opposing views.

The risks against the absolute right to hold a belief is simply not acceptable. Technology that identifies or infers emotions or thoughts of natural persons manipulates these persons or induces their self-monitoring. Such impact contradicts the right to hold a belief, which is an absolute right. Consequently, these technologies cannot be used without informed consent of the people concerned, including in the pursuit of internal security or for purposes of crime repression.

Risks linked to errors and to the theft of biometric identifiers are numerous.

Technical errors are common. Technology can be liable to falsely recognise or authenticate a person (in this latter case, it is called *"false match"*), or to not recognise or authenticate a person where it should (a *"false non-match"*). A striking example of errors due to a false match is provided by an independent report, which concludes that the facial recognition system used by the London Metropolitan Police is *"verifiably accurate in just 19% of cases"*, which means that *"81% of 'suspects' flagged by [the] technology [are] innocent"*.

Human-based errors and weaknesses are also common. The construction of the categories used to detect, evaluate, or classify persons is human-based and subjective, and errors may arise. The way in which technology is implemented may itself lead to unwanted impacts, such as the reinforcement of stereotypes. It might also be argued that the choice of biometry and video-surveillance to fulfil a purpose of security is, in itself, a human-based course error. Indeed, biometric identification does not bring any security. It only enables, eventually, the identification of persons already suspected of preparing an offence. It might be the reason why biometric research focuses on prediction. However, in a democratic society governed by the rule of law, the restriction of a freedom based on a prediction of behaviour is not admissible. It constitutes, per se, a violation of the right to hold a belief, of the freedom of self-determination, and of the freedom of free will. In the end, it constitutes a violation of human dignity. This principle also applies to the industry.

Risks of theft of biometric identifiers are also high. Biometric data may be vulnerable to risks at four levels. At the individual level, the theft of fingerprints or of facial characteristics is quite easy, and this is increasingly documented. Biometric identifiers can also be intercepted when they are captured, transmitted, or compared with the main database. In standard authentication systems, if basic rules of security are implemented, the impact of a theft at these last three levels is generally quite reduced. Whereas conversely, the theft of a biometric identifier can be highly impactful. Indeed, this identifier is reusable, by design, on every other biometric-based system, in the pursuit of numerous purposes, without the person concerned necessarily being aware of such wrongful use.

Risks of errors and theft induce a practical reversal of the burden of proof. Technology-based and human-based errors are particularly worrying in relation to biometric identifiers because these identifiers

are presented as highly reliable. The victim of a misidentification may therefore have, in practice, to demonstrate the mistake. However, under the ECHR legal system, the burden of demonstrating the necessity and proportionality of a restriction of freedom is borne by the party responsible for imposing the restriction. The reversal of the burden of proof violates the ECHR.

Risks of errors and theft impact the right to a fair trial and the right to human dignity. Firstly, the monitoring of publicly accessible places negates the presumption of innocence, since it leads to stigmatising, by default, any individual as a suspect. Yves Poullet also observes that such a negative representation of the human being may ultimately induce behaviours that will then justify the surveillance practices. This would directly hurt human self-determination and human dignity. In addition, the use of this technology negates the principle that offences and penalties must be defined by law, because the factors being monitored are generally not known. Finally, the use of biometric identifiers has impacts on dignity because it induces the possibility that a large number of persons will access these identifiers, thus depriving the individual of the possibility to choose by whom and why their identifiers can be used. This takes place in a context where any single undue access might have terrible consequences, because the identifier cannot be revoked, and where the mismanagement of existing public national and European biometric databases has been proven.

The use of biometric identifiers for purposes of security, and more precisely to fight terrorism and manage borders, also impacts the very credibility of the fight against terrorism. Indeed, it results in the discrimination of persons based on their nature, character, appearance, social origin, or ethnicity. There is an explicit contradiction in combatting terrorism in the name of values that include the right to non-discrimination, using discrimination based on ethnic and social characteristics. François Sureau further highlights that the disproportionate restriction of freedoms in the name of combatting terrorism offers terrorists *"a victory without a struggle, because it shows how weak our principles were"*. These contradictions undermine the credibility of the fight against terrorism in the name of European values.

The use of biometric mass surveillance technology ultimately induces a risk for democracy itself. Primarily, it induces a possibility of abuse that was never reached in history. This threatens the rights to self-determination and to human dignity, which suffer no limitation in a democracy governed by the rule of law, since they already constitute the core of fundamental rights that must be respected under any circumstances. Notwithstanding those circumstances, the European Union and several member states turn a blind eye and a deaf ear to the legal analyses, opinions from data protection authorities, and court decisions that highlight the unacceptability of practices. This might constitute a clear signal of an unacceptable *"paternalistic 'best interests' decision-making"* attitude to quote the ECtHR, which would itself be unacceptable.

One of the most obvious impacts this situation generates is the risk of disappearance of the right to resist oppression. This was notably highlighted by one hundred and twenty members of the French Parliament in 2012, in relation to the creation of a central biometric database, referred to as *"the file of honest people"*. In essence, such disappearance would mean that liberal democracy itself has already disappeared. It would mean that the core of fundamental rights has itself disappeared – based on the denial of the democratic constitutive elements that are the requirements for necessity and proportionality of any limitation of right.

SECTION 6 RECOMMENDATIONS

The current analysis leads to four recommendations that seem basically undisputable if the European Union and its member states intend to stay on a democratic path. They can be summarised as follows.

1) CONVENE A GENERAL FORUM ON DEMOCRACY, HUMAN RIGHTS, AND THE RULE OF LAW

Proper protection of human rights implies that assessments of necessity and proportionality on one hand, and risk assessments on the other, are properly conducted. This also implies that the law passed to base practices complies with the requirements of legitimate and clear legal basis. This can only be ensured in states where democratic checks and balances are effective. Currently, it seems not to be the case, both at the level of the institutions of the European Union and at the level of some EU member states.

Consequently, it appears crucial to conduct an effective assessment of the proper democratic functioning of the European institutions and of the EU member states, and to ensure that the latter undertake the reforms necessary to restore effective checks and balances and comply with the rule of law. In particular, parliaments must have an effective law-making power and must not be circumvented. Courts must be independent and their rulings must be enforced. Data protection authorities must have effective supervisory and decision-making powers and their opinions must be enforced as well. All these authorities and institutions must be adequately equipped and resourced to carry out their missions.

2) RESTORE THE CONDITIONS FOR DEMOCRATIC DEBATE

In a political democracy, states must ensure that the best contextual parameters are set up to enable public debate. They must also ensure that contradictory opinions are considered.. Public authorities and political representatives bear special responsibility for ensuring that they act according to citizens' choices, particularly where voices are speaking out about a risk for absolute fundamental rights.

Restoring the conditions for democratic debate also implies avoiding any misrepresentations of reality, including in relation to the actual content of the legal provisions that underpin human rights preservation. Manipulation of opinion polling must be prohibited, and the form of public communication itself should stigmatise neither minorities nor the authorities and persons who question the legitimacy of proposals from the government. Codes of conducts for political and public representatives might be envisioned to promote such *"ethics of communication"* (Venice Commission).

3) IMPLEMENT HUMAN RIGHTS EDUCATION IN SOCIETY AND IN THE POLITICAL SPHERE, AT NATIONAL AND EUROPEAN UNION LEVELS

Democracy requires citizens to understand what legislation and practices really imply. This notably requires providing citizens with the skills and critical attitude that enable them to face and understand the information they receive. This right to education is of particular importance and has been especially highlighted by the Council of Europe Committee of Ministers as well as by the European Parliament.

A culture of human rights must also be fostered amongst political and public representatives, at national levels and the level of the European Union. In a democratic society governed by the rule of law, it is not acceptable that these representatives make statements and take actions that directly contradict the letter and philosophy of the texts that preserve human rights. These practices and statements demonstrate a lack of a culture of democracy and human rights.

The understanding of the letter and philosophy of preservation of human rights should also pervade Privacy and Data Protection Impact Assessments (respectively PIA and DPIA), which currently often reduce the necessity and proportionality assessment to a check of compliance with the GDPR or the Police-Justice Directive.

4) DECLARE AN IMMEDIATE MORATORIUM ON TECHNOLOGY AND PRACTICES THAT IMPACT THE RIGHT TO HOLD A BELIEF, THE RIGHT TO SELF-DETERMINATION, THE RIGHT TO HUMAN DIGNITY, AND THE RIGHT TO RESIST OPPRESSION

Several usages of biometric identifiers constitute a violation, or induce intolerable risks against a series of absolute rights such as the right to hold a belief, the right to self-determination, the right to human dignity, and the right to resist oppression. This situation leads to a risk for liberal democracy as a political regime. Consequently, it is crucial to ban these practices, during the time required to build the underlying conditions for their democratic assessment, to conduct this assessment and to submit its results for proper public debate.

Most dangerous data processing methods could be discriminated from other methods based on the three following criteria: (1) the proximity of the data storage to the person concerned; (2) the existing possibilities to reuse the biometric identifier for other purposes; and (3) the accuracy of biometric identifiers.

Technologies and practices that must be banned as a first step include:

(1) The collection and processing, by states and by the institutions of the European Union, of biometric identifiers relating to all citizens on the one hand and to all migrants on the other hand, without further necessary and proportionate discrimination based on justified real and crucial needs.

(2) The collection and processing, by private entities, of biometric identifiers without the freely given, specific, explicit, and informed consent of the people involved. This covers the collection of photographs and other biometric identifiers that are publicly available or available on the Internet.

(3) Facial recognition in publicly accessible places.

(4) Biometric and behavioural recognition and classification without the freely given, specific, explicit and informed consent of the people concerned. In addition, these technologies must not lead to taking decisions against the persons involved or any other human being without a consent of a similar nature from the people concerned or involved.

In any and all situations, authorised technologies and services should be subject to a proper privacy impact assessment, and the person responsible for them should be able to demonstrate that findings of this assessment, in terms of corrective measures and guarantees, were implemented and will be regularly subject to independent supervision.

SECTION 8 CONCLUSION

For nearly twenty years, biometry has been shown as the unquestionable way to ensure people's security, both in the public and in the private spheres. On this basis alone, European countries are implementing increasingly intrusive technology, without ever having been able to demonstrate its efficiency and added-value, despite continuous requests for evidence.

Conversely, an analysis of the issues at stake demonstrates important risks of fraud as well as technical and human-based errors, which are further illustrated by practical examples. These observations take place in a context where the mismanagement of existing public national and European databases has been proven. In addition, a rigorous legal study articulates intolerable risks to rights and freedoms that are the foundations of any political democracy caring about respecting its members. In particular, it is demonstrated that a simple biometric identifier theft or a diversion of processing purpose may have very serious impacts on individuals, in addition to affecting their dignity based on a non-consensual processing of some of their more intimate data.

The actual reasons for this Kafkaesque situation are unclear. The biometric industry's lobby undoubtedly comes into play, and it is certainly compounded by the temptation, inherent to any state, to ensure internal order. Either way, this situation is made possible by the weakening of democratic checks and balances and a distortion of public communication, which seeks acceptability to the detriment of justification. This may be observed both in the European Union member states and within the institutions of the European Union. In other words, this situation is the result of the practical abandonment of the principles that all member states pledged to respect after the Second World War within the Council of Europe to prevent any reoccurrence of a totalitarian regime.

The member states of the European Union now find themselves confronted with a crucial political choice. The choice to rediscover the principles and values of the rule of law and the respect of human rights, or the choice to stray from this path and go down the road to totalitarianism. Such a statement is not exaggerated, it is result oriented. It will be understood by anyone who looks at history and is conscious of the relevance and the value of the principles transmitted to us by the writers of the European Convention on Human Rights. It will be understood by anyone reading the calls to prohibit biometric technology from almost all democratic residual checks and balances: the United Nations, the European Parliament, Data Protection Authorities, and the NGOs that work on a daily basis to preserve Human Rights.

The later this decision is made, the more difficult it will be to implement, when all the technological means are in place.

To borrow the words[1] pronounced over 20 years ago by the current President of the Council of the Bars and Law Societies of the European Union (CCBE), the question put to states and to the institutions of the European Union is whether they are capable of demonstrating their *"democratic maturity"*. More specifically, the question is to know whether they *«acknowledge the primacy of the Human being"* or if they are demanding *«its submission»*. The answer to this question, in relation to the arguments to be opposed to terrorism, will undoubtedly be decisive.

Footnotes

1. *Michel Bénichou, « Le résistible déclin du secret », LPA, 20 juin 2001, no122, p. 3 s.*

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