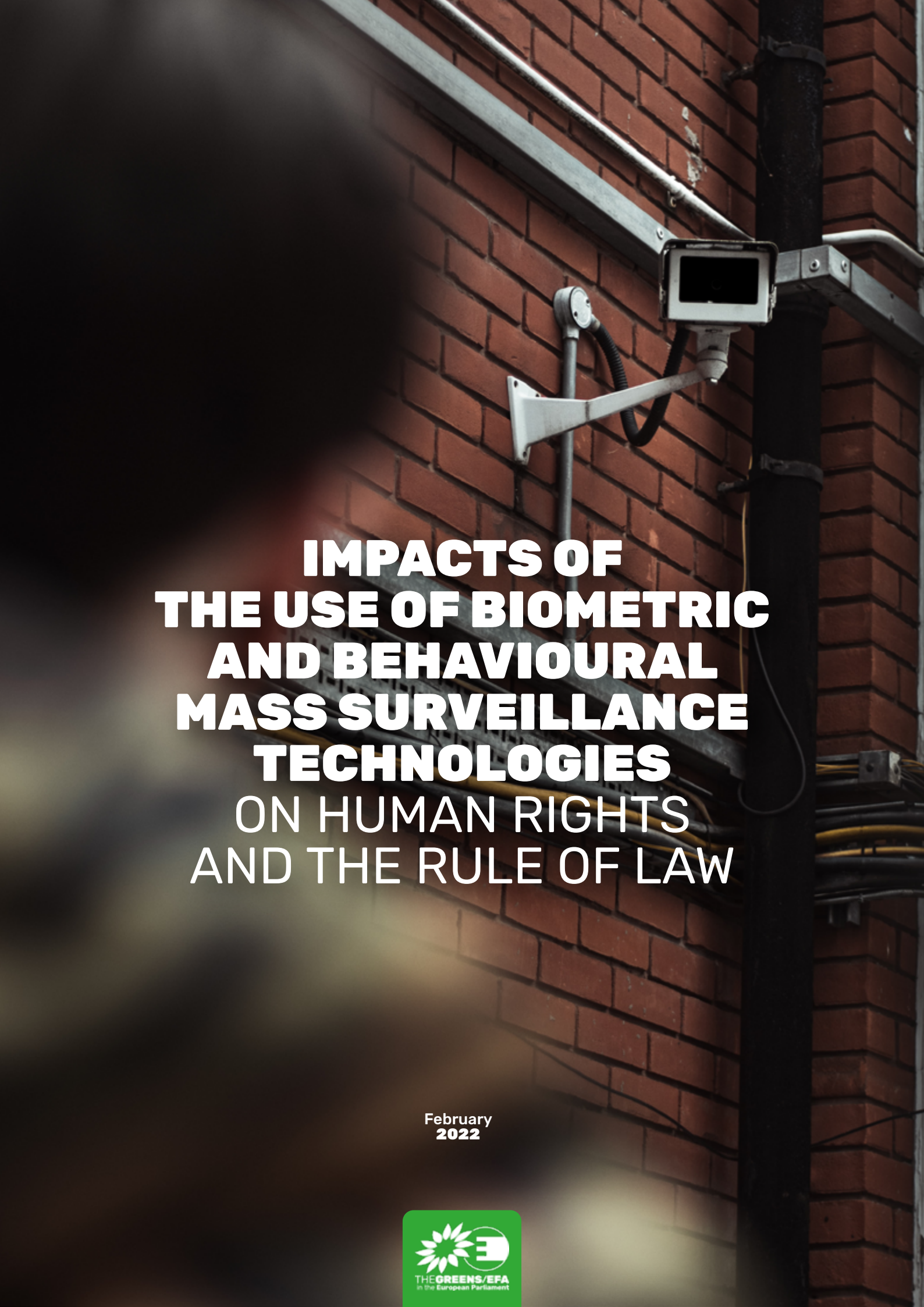

IMPACTS OF THE USE OF BIOMETRIC AND BEHAVIOURAL MASS SURVEILLANCE TECHNOLOGIES ON HUMAN RIGHTS AND THE RULE OF LAW

February
2022

THE GREENS/EFA in the European Parliament

ABSTRACT

Public authorities justify the implementation and further development of biometric and behavioural technology as a need that requires no discussion, in order to fight terrorism and ensure security. However, so far they have failed to bring evidence of efficiency and added-value, and they appear to circumvent any serious debate on the very principle of prohibiting this technology. Despite this position, an impact analysis articulates intolerable risks to rights and freedoms that are the foundations of any political democracy that cares about respecting its individual members. In particular, it is demonstrated that biometric identifier theft or diversion of the processing purpose may have very serious impacts on individuals, along with affecting their dignity based on a non-consensual processing of one of their more intimate data. This occurs in a context where the mismanagement of existing biometric databases by institutions of the European Union and some member states has already been demonstrated.

Consequently, the member states of the European Union find themselves confronted with a crucial political choice. They can chooseto rediscover the principles and values of the rule of law and the respect of human rights, and to ban the use of biometric identifiers and of biometric recognition, at the very least in publicly accessible places. Or they can choose to stray from this path and go down the road to totalitarianism, by keeping their current trajectory. Such a statement 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 also be understood by anyone aware of the calls to prohibit facial recognition from almost all residual democratic checks and balances, including the United Nations, the European Parliament, and Data Protection Authorities.

The answer to this choice, in relation to the arguments to be opposed to terrorism, will undoubtedly be decisive.

AUTHORS AND CONTRIBUTORS

Authors
Estelle De Marco
Aeris

Contributors
Célie Zamora
Valentina Pavel

Linguistic proofreading
Mireille Renaud-Mallet

TABLE OF CONTENT

ABSTRACT 2

AUTHORS AND CONTRIBUTORS 3

TABLE OF CONTENTS 4

LIST OF MAIN ACRONYMS AND ABBREVIATIONS 8

1. EXECUTIVE SUMMARY 10

2. INTRODUCTION 21

2.1 CONTEXT OF THE STUDY 22
2.2 PURPOSE AND STRUCTURE OF THE STUDY 25
2.3 SCOPE AND DEFINITIONS 26
2.4 METHODOLOGY 27

3. CONTOURS AND CONTENT OF THE USE OF SURVEILLANCE TECHNOLOGIES 33

3.1 CURRENT USE OF MASS SURVEILLANCE TECHNOLOGIES WITHIN THE EU & WESTERN BALKANS 34
1. Use, by public authorities, of biometric mass surveillance technologies 34
2. Other usages of surveillance technologies 36
3.2 THE ROLE OF EUROPEAN AND NATIONAL ACTORS IN THE FIELD 37
3.3 CIVIL SOCIETY RESPONSES 40

4. THE LEGISLATION REGULATING SURVEILLANCE 53

4.1 THE ECHR AND THE EUCFR REQUIREMENTS 54
1. Respecting human rights and the rule of law: a societal choice implying more than formal statements 54
2. Fundamental rights impacted by the use of mass surveillance technologies 55
1. The right to private and family life 55
2. The right to the protection of personal data 56
3. The right to freedom of expression 57
4. The right to freedom of assembly and association 57
5. The right to freedom of opinion 58
6. The right to freedom of movement 58
7. The right to liberty and security 59
8. The right to non-discrimination 59
9. The right to education 60
10. The right to a fair trial and related rights 60

11. The right to dignity and to self-determination 61
12. The right of resistance to oppression 63
3. The conditions for limiting fundamental rights in a democratic society governed by the Rule of Law 64
1. The requirement for a determined and legitimate purpose 64
2. The requirement for efficiency 65
3. The requirement for minimisation 65
4. The requirement to set-up guarantees 66
5. Further restrictions to the possibility to limit a fundamental right: particularly protected rights, prohibition to suppress a right, and right to dignity 66
4.2 EUROPEAN UNION LEGISLATION 69
4.3 NATIONAL LEGISLATIONS 72

5. IMPACTS OF THE USE OF MASS SURVEILLANCE TECHNOLOGIES ON HUMAN RIGHTS 90

5.1 THE SOURCES OF IMPACTS ON HUMAN RIGHTS 91
5.2 ASSESSMENT OF THE COMPLIANCE OF THE USE OF MASS SURVEILLANCE TECHNOLOGIES WITH THE REQUIREMENT FOR NECESSITY AND PROPORTIONALITY 92
1. Lack of clarifications in relation to purposes and their legitimacy 92
1. Lack of purposes specification in relation to practices 92
2. Lack of specification of purposes in specific legislation 93
3. Purposes diversion 94
4. Failure to specify the legitimacy of purposes 94
2. Issues relating to the principle of efficiency 95
3. Issues relating to minimisation 96
4. Issues relating to the principle of legal basis and transparency 97
1. Lack of appropriate legal basis 97
2. Lack of effectiveness of Parliaments decision-making power 98
5. Lack of other guarantees 100
6. Conclusion of the necessity and proportionality assessment 101
5.3 RISKS FOR HUMAN RIGHTS 102
1. Risks for the right to private life 102
1. Disproportionate loss of opacity for the individual 102
2. Unjustified loss of personal development and of personal autonomy 102
3. Genuine, current and serious threat to self-determination and to dignity 103
2. Risks for the right to freedom of expression and of assembly 103
3. Risks for the absolute right to hold a belief 104
4. Risks linked to errors and theft 105
1. Technology-based errors 105
2. Human based errors and weaknesses 105
3. Risks of theft 106

4. Impacts in terms of reversal of the burden of proof 107
5. Impacts on the right to a fair trial and on human dignity 108
6. Impacts on the credibility of the fight against terrorism 108
5. Risk for democracy 109
1. A possibility of abuse that was never reached in history 109
2. The circumvention of democratic checks and balances 109
3. A clear signal of unacceptable paternalistic decision-making approach 110
4.The risk of disappearance of the right to resist oppression 110
5. The need to settle the proper conditions for understanding and debating democracy and preservation of freedoms 111
6. The need to put an end to the misrepresentation of reality 111

6. RECOMMENDATIONS 124

6.1 CONVENE A GENERAL FORUM ON DEMOCRACY, HUMAN RIGHTS, AND THE RULE OF LAW 125
6.2 RESTORE THE CONDITIONS FOR DEMOCRATIC DEBATE 126
6.3 IMPLEMENT HUMAN RIGHTS EDUCATION IN SOCIETY AND IN THE POLITICAL SPHERE, AT NATIONAL AND EUROPEAN UNION LEVELS 127
6.4 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 128

7. CASES STUDIES 132

7.1 FRANCE 132
1. State of use of surveillance technologies 133
1. Current offline use, by public authorities, of biometric and behavioural mass surveillance technologies 133
2. Other usages of surveillance technologies 135
3. Political standing in relation to the use of mass surveillance technologies 137
2. Legislation regulating mass surveillance technologies 138
3. Civil society responses 139
7.2 THE UNITED KINGDOM 139
1. State of use of surveillance technologies 139
1. Current offline use, by public authorities, of biometric and behavioural mass surveillance technologies 139
2. Other usages of surveillance technologies 140
3. Political standing in relation to the use of mass surveillance technologies 140
2. Legislation regulating mass surveillance technologies 141
3. Civil society responses 143

7.3 ROMANIA 146
1. State of use of surveillance technologies 146
1. Current offline use, by public authorities, of biometric and behavioural mass surveillance technologies 146
2. Other usages of surveillance technologies 148
3. Political standing in relation to the use of mass surveillance technologies 149
2. Legislation regulating mass surveillance technologies 150
3. Civil society responses 151

8. CONCLUSION 166

9. ANNEX 1 – LACK OF LEGITIMATE BASIS OF LEGAL INSTRUMENTS THAT ORGANISE THE POSSIBILITY OF MASS BIOMETRIC RECOGNITION 168

9.1 ABSENCE OF LEGITIMATE LEGAL BASIS OF THE EU REGULATION 2019/1157 ON STRENGTHENING THE SECURITY OF IDENTITY CARDS 169
9.2 ABSENCE OF LEGITIMATE LEGAL BASIS FOR A PROPOSED ARTIFICIAL INTELLIGENCE REGULATION 170

LIST OF MAIN ACRONYMS AND ABBREVIATIONS

ANSPDCP	Romanian Data Protection Authority
CCTV	Closed-Circuit Television (refers to video-surveillance)
CNIL	French Data Protection Authority
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
EUCFR	European Union Charter of Fundamental Rights
EUCJ	European Union Court of Justice
EUR	Euros
GDPR	General Data Protection Regulation
ICO	The United Kingdom Data Protection Authority
LEAs	Law Enforcement Agencies
NGOs	Non Governmental Organisations
USA	United States of America

1

EXECUTIVE SUMMARY

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.*

2
INTRODUCTION

2.1 CONTEXT OF THE STUDY

In 1516, Thomas More described in his book *"Utopia"*[1], a world marked by discipline and strong social control. In this world, the monitoring of individuals extended to most aspects of their private and public lives[2]. *"Utopia"* was interpreted differently depending on the period and philosophical sensitivities of readers[3], but it is considered one of the first publications that raised the question of the totalitarian nature of states that monitor and regulate activities of citizens in such a way that this monitoring prevents any serious opposition, resulting in the inability for individuals to enjoy their freedoms and express their free will[4]. From the 16th century to the 21st century, several other literary authors[5] and political philosophers such as Alexis de Tocqueville[6] described or criticised similar social organisations in their respective publications.

This literature has developed alongside growing awareness amongst the European population of the link between social control and limitation of freedoms, which is partly reflected in the analyses of historians who studied the *"rationalisation of administrative surveillance"*[7]. John Torpey, especially, studied the *"administrative efforts to control the movement of persons in modern territorial states and across borders"*[8] using identification documents. He analysed first the 1789 French revolution, during which a temporary administrator of the city of Paris, named Peuchet, declared the obligation made to citizens to hold passports in some contexts *"contrary to all principles of justice and of reason"*, because this practice was depriving individuals of their right *"to breathe the air [they choose] without having to ask permission to a master who can refuse [them] that right"*[9]. Peuchet considered that the French state was operating *"surveillance as extensive as it is dangerous"*, evoking a *"slavery of passports"*[10]. At the same time, the former regime's practice of *"systematic registration"*[11] of certain categories of individuals, with the aim of monitoring them, was also criticised for being *"summary, secret and free from traditional court proceedings"*[12].

During the 18th and the 19th centuries, the issue of surveillance became the subject of further publications of a philosophical and sociological nature.[13] In particular, the lawyer and philosopher Jeremy Bentham, in his book *"The Panopticon Writings"*, imagined in 1787 an *"ideal prison"* whose architecture would enable a watchperson to monitor everyone without being seen.[14] Since *"The Panopticon Writings"* was analysed by the philosopher Michel Foucault in his own book *"Discipline and Punish"*, published in 1975[15], Jeremy Bentham is considered the *"inventor of a perfect process for surveillance"* called *"Panopticon"*, and his book is considered as one of the founding texts of the debate on surveillance.

At the same time, Albrecht Funk observed that *"beyond the high ground of liberal demands for free movement, the state administration and the police in France, Germany, as well as in Britain, relied on a multitude of laws and regulations, permits and identity papers which aimed at the surveillance and control of the movements of certain segments of the population (servants, workers, artisans, gypsies, the Sachseng nger in Prussia"*[16], slaves or workers employed in the British North-American colonies[17]. In France, these controls were partly based on the written *"description"* of persons under surveillance[18]. The development of photography led police services to progressively use it in addition to these *"descriptions"*, in order to identify those suspected of being involved in criminal activity, and then to identify those considered to be mentally incapacitated and political opponents.

By the end of the 19th century, French public opinion considered that such collection of photographs was *"an intolerable threat to individual freedoms which should not be imposed on honest people"*[19], echoing the criticism expressed towards passports during the previous century. Indeed, all these criticisms appear to express a similar fear: the actual denial of one or more freedoms based on the use of identification documents, or, in other words, the possibility for public authorities to choose, potentially arbitrarily depending on contextual political choices[20], the individuals considered as belonging to the category of *"honest people"* and those considered as not belonging to that category and who may, as a consequence, suffer some restrictions to their freedom on the sole ground of such categorisation.

The main concern appears therefore to be that, in a context of generalised surveillance, citizens feel unable to anticipate the purposes for which identification techniques might be used against them, and thus find themselves unable to regulate their conduct accordingly in order to be classified as *"honest people"*. In addition, they might very well also be obliged, to this end, to modify personal conducts they otherwise deem legitimate.

These same concerns had led several sociologists and philosophers, during the 18th and the 19th centuries, to propose the guiding principles of a new judicial system. In particular, Cesare Beccaria proposed in 1765 several principles which later inspired international legal instruments currently protecting human rights[21]. According to Beccaria, clear laws should precisely define offences and penalties[22], penalties should be proportionate to the offence[23], and the purposes of limitations of freedoms should actually be useful and not based on *"a danger imagined or of minor importance"*[24].

At the end of the 19th century, the strong reservations from civil society about photographs, combined with the relative efficiency of photograph to accurately identify people[25], slowed down the proposal to establish identity cards. At the same time, the French police officer and biometrics researcher Alphonse Bertillon developed an anthropometrical identification technique, drawing from previous works on the physical classification of individuals in France and in Belgium, led in the latter country by the mathematician Adolphe Quetelet[26]. Bertillon's technique was based on distinctive signs and fingerprints as well as photographs. It is considered to be a predecessor to the current systems of biometric identification, together with some substantial modifications contributed by the English scientist Francis Galton, who proposed a mechanical ranking method based on measurements of the human body[27], and other anthropological research focussing on different parts of the human body, especially *"the field of view or the iris colour"*[28].

These techniques were used in judicial matters in several countries across Europe[29] and beyond, such as in Argentina, where an anthropometric department was inaugurated in Buenos Aires in 1889[30]. These identification techniques were also used in colonial empires against a backdrop of protests, especially from *"colonised people in Indochina [who] denounced an oppressive disciplinary practice on multiple occasions"*[31]. These techniques were further improved based on works on ranking and transmission methods, especially of a digital nature[32].

From the late 19th century to the First World War, the sociologist and historian John Torpey reports that there was a recrudescence of *"various kinds of identification documents that sharpened the line between national and aliens"*[33], especially in Italy, France and Germany, in addition to the United States[34]. From the First World War on, *"documentation surveillance"* was intensified and, in some countries, was extended to nationals or to some categories of nationals.[35] For example, identity documents became mandatory for foreigners in France and for all residents in Germany and in Italy.[36] In several countries, most of these measures remained in effect in the inter-war years and were further intensified before or during the Second World War.[37] Identity cards became mandatory in 1940 in France[38], while Germany was already practicing *"surveillance and classification in order to privilege 'Aryans' and to eliminate"*[39] minorities that were regarded as undesirable such as Jews, homosexuals, and Gypsies as well as *"groups outside German borders that were deemed inferior in the racial hierarchy, such as Slavs"*[40]. This sorting process was facilitated by the use of *"IBM Hollerith punch-card machines"*[41], which were also in use in France in order to puncture identity documents of Jews and identify them easily[42]. Similar surveillance and systematic identification practices were in use a little later in South Africa under the Apartheid regime ([1948–1993])m where *"personal history and movements of every African worker"* was linked to *"fingerprint-based ID cards"*.[43]

Identity cards survived the war in France, Italy, and Germany[44]. They were abolished in 1952 in the United Kingdom, after a court ruled that they could, during peacetime, *"antagonise the relationship between the citizenry and the police"*[45]. Indeed, the establishment of mandatory identity cards questions *"the very foundations of the relationship between the individual and the state"*[46] and, in relation to France, the fact that such obligation occurred in a context of *"almost total deprivation of liberty"*[47], after unsuccessful attempts to enforce it during peacetime, and was not abolished after the war, may reveal a political will to establish control over citizens, against the will of the majority of them. This conclusion, partly drawn by the specialised journalist Olivier Tesquet, concurs with the analysis of Christopher Dandeker, professor of Military Sociology. According to David

Lyon, Christopher Dandeker considers that *"the state's supervisory powers over society extended in order to facilitate military objectives, something that became even more clear as 'welfare states' were created after World War II"*[48]. Under this approach, *"the military-surveillance connection will persist"* as long as *"the existence of bureaucratised and technologized military power is seen as a mean of maintaining peace"*.[49]

In 1950, in order to prevent a return to totalitarianism, the representatives of the Council of Europe member states signed the European Convention on Human Rights (ECHR), which established a series of fundamental rights derived from the United Nations' 1948 Universal Declaration of Human Rights[50] and from the rules expressed by Beccaria (which are based more generally most international texts establishing fundamental rights[51]). As a result, the ECHR requires at the 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 (principles of necessity and proportionality)[52].

From 1970 onward, the ongoing digitisation of data collected about citizens led to the adoption of more specific legislation on the use of personal data, in several countries. The first data protection law was adopted in the German State Hessen in 1970 (Datenschutzgetsetzgebung)[53]. Other similar laws were adopted across Europe, including in Sweden in 1973[54], in Germany as a federal State in 1977, in France, Austria, Denmark and Norway in 1978, and in the United Kingdom in 1984[55].[56] In 1981, the Council of Europe opened to signature Convention 108 for the protection of individuals with regard to the processing of personal data (amended in 2018)[57]. In 1995, the European Union adopted Directive 95/46/EC, aiming at protecting *"the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data"*[58] (this Directive was repealed and replaced in 2018 by the General Data Protection Regulation - GDPR)[59].

At the same time, during the 1990s, structured studies emerged for the purpose of providing a theoretical framework and methodologies enabling the rigorous analysis of surveillance.[60] Under the impulse provided by the authors of these studies, primarily by sociologist David Lyon and the researcher Gary T. Marx, the analysis of surveillance became an interdisciplinary research field called *"surveillance studies"*, which, however, represents only one part of theories of surveillance and of the latter's implications.[61]

From 1985 on, genetic fingerprinting also emerged from new findings on DNA, and police departments started using genetics, followed by facial recognition.[62] These techniques were further exported from the field of criminal justice to different social uses.[63] Over the last twenty years, there has been an exponential increase in the development of digital applications and associated personal data collection by diverse stakeholders for a wide variety of purposes. In this context, the concerns of civil society have also continued to grow, with a particular emphasis on security considerations.[64] In recent years, the increased use of biometric and behavioural identification around the world[65], as well as the strengthening of the investigatory and surveillance powers of law enforcement agencies and intelligence services[66], have been justified as tools to ensure security, fight terrorism, and combat the Covid-19 global health pandemic[67]. In that respect, two legal authors observe that biometry *"can be regarded as a new significant step in the process of streamlining and improving identification procedures and instruments"*.[68]

Nowadays, civil society and politicians alike are calling for an end to this culture of identification and control[69], which is widely considered a threat to democracy and the rule of law[70]. These fears are often combined with a general mistrust of public representatives, who intensify the implementation of surveillance measures despite the widespread opposition from citizens, and without any engagement in serious debate[71]. On the other hand, public representatives and institutions appear to cultivate the opacity of data processing practices[72] and to justify surveillance using false arguments or reasoning.[73]

In this context, it is essential to frame the terms of 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 mass surveillance technologies. If this is the case, we must explore to what extent and by which types of technology. Within the framework of this analysis, there is also a need to understand the very meaning of the concepts of 'human rights' and 'the rule of law'.

2.2 PURPOSE AND STRUCTURE OF THE STUDY

The purpose of the current study is to identify the impacts of the use of biometric and behavioural mass surveillance technologies in Europe on human rights and the rule of law, with a focus on the practices of public authorities.

To this end, this study includes a brief overview of the current state of play in the use of such technologies in Europe, as well as an outline of the different kinds of technology in use. The study also includes a summary of the legal framework that regulates the use of such technologies, in addition to an analysis of the ways in which these technologies impact on human rights and on the rule of law. This was carried out through a fundamental rights impact assessment. Three country examples are offered at the end of the report: France, the United Kingdom, and Romania.

2.3 SCOPE AND DEFINITIONS

The concepts of *"fundamental rights"* or *"fundamental freedoms"* is understood as referring to rights and freedoms that belong to individuals (natural persons) and legal entities, and that are protected against both the executive and the legislative powers, based not only on national law but also on the Constitution or on international legal instruments, and that are enforced not only by national judges but also by constitutional and even international judges[74]. This concept of fundamental rights and freedoms is more recent than the concept of *"civil liberties"*, which refers to rights and liberties that are ensured, at a national level, against the executive power[75], generally in the Constitution. Fundamental rights and civil liberties may both be seen as *"a form of legal consecration of Human Rights"*[76]. Indeed, the concept of Human rights refers to rights that are *"inherent in the Human Being"* in the sense that they are *"considered to naturally belong to each Human Being"*[77].

The concepts of *"human rights"* and of *"fundamental rights"* or *"fundamental freedoms"* will be treated as synonymous within the framework of the current study, unless stated otherwise, because the human rights under scrutiny are also fundamental rights and freedoms established in the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and in the European Union Charter of Fundamental Rights (EUCFR).

The concept of the *"rule of law"* can be defined as a system where *"all persons and authorities within the state, whether public or private, should be bound by and entitled to the benefit of laws publicly made, taking effect (generally) in the future and publicly administered in the courts"*.[78] The Venice Commission of the Council of Europe considers that the necessary elements of the rule of law are (1) Legality, including a transparent, accountable and democratic process for enacting law;

(2) Legal certainty; (3) Prohibition of arbitrariness; (4) Access to justice before independent and impartial courts, including judicial review of administrative acts; (5) Respect for human rights; and (6) Non-discrimination and equality before the law.[79] The Venice commission also published a *"rule of law checklist"* that is intended *"to provide a tool for assessing the Rule of Law in a given country from the view point of its constitutional and legal structures, the legislation in force and the existing case-law. The checklist aims at enabling an objective, thorough, transparent and equal assessment"*.[80] Indeed, the Commission *"warned against the risks of a purely formalistic concept of the Rule of Law"* and *"stressed that individual human rights are affected not only by the authorities of the State, but also by hybrid (State-private) actors and private entities which perform tasks that were formerly the domain of State authorities, or include unilateral decisions affecting a great number of people, as well as by international and supranational organisations"*. As a result, the Commission *"recommended that the Rule of Law principles be applied in these areas as well"*.[81]

Online surveillance technologies are outside the scope of the current study, as well as surveillance practices that do not fall within the definition of biometric mass surveillance, insofar as these surveillance activities are not linked or do not amplify the impact of member states' offline surveillance activities.

The notion of *"mass surveillance technologies"* is understood as technologies, which, depending on the way they are used, may enable mass surveillance. A common characteristic of such technologies is to enable mass surveillance in certain contexts, even though they are not implemented in that particular purpose.

The notion of *"surveillance"* is understood as *"watching over"*[82] or *"all the acts by which an ongoing check is exercised"*. The notion of *"watching over"* is understood as *"watching with particular attention*[83]*, so as to exercise a control or a verification"*[84] in a variety of possible purposes such as *"influence, management, protection or direction"*[85].

In the context of the use of electronic and computing technologies, taking into account the definition of electronic surveillance[86], the notion of *"surveillance"* applied to individuals refers to the attentive watch or recording of data relating to a person's activity or behaviour, or relating to specific activities or behaviour of the person, so as to enable control or verification, even at a later stage after the recording itself.

The notion of *"mass surveillance"* is understood as the application of surveillance activities to an entire group of persons. This is clarified as persons in that group who are connected through a criterion that is not the one that motivates surveillance[87]. In this way, any member of that group could be identified, even though such identification would need to resort, to additional technologies or techniques. In this context, the notion of *"identification"* includes the possibility to give a *"recognisable identity"* to an individual, and the ability to identify or recognise this individual through their movements, acts, relationships, preferences, habits, behaviours, and mobility[88]. The notion of biometric surveillance is understood as a surveillance that relies on the processing of biometric identifiers, which is data related to physical or physiological aspects of the human body,[89] including non-exhaustively retina or iris scan, voiceprint, scan of hand, face geometry, DNA, finger and palm print"[90]. Biometric surveillance may have different purposes, ranging from identification to detection through to categorisation[91].

The notion of behavioural surveillance is understood as surveillance that relies on the processing of characteristics or *"conditions of a […] behavioural, psychological or emotional nature"*[92], including non-exhaustively *"keystroke or mouse dynamics, gesture dynamics, signature dynamics, […] voice and gait feature"*, body signals and machine usage and interaction.[93] Behavioural techniques are considered to be biometric techniques of a *"weaker"* or *"softer"* kind[94] and are sometimes referred to as *"behaviometrics"*[95]. Some new techniques further enable *"the capture of entirely new types of bio-signals, such as heart beats and brain waves via EEG or ECG, and the development of brain-computing-interfaces (BCI) [which] measure neuro activity and translate brain activity into machine-readable input"*. To some extent, these technologies can enable the detection of thoughts or intent.[96]

SUMMARY OF DEFINITIONS

The concept of human rights refers in the current study to rights that are inherent to human beings, and which have been established as fundamental rights and freedoms by international legal instruments. As a result, they are protected against both the executive and legislative powers, and they are enforceable by national and international judges.

The notion of surveillance corresponds, as a minimum, to the ability to control, at a given time or at any time (depending on whether surveillance is direct or consists of a data recording), what those who implement it or access it want to detect, for a variety of potential purposes (whether the purpose is or not defined at the time surveillance is ongoing), through attentive watch or recording. Surveillance is deemed *"mass surveillance"* where it concerns a vast number of persons who are connected through a criterion that is not the one that motivates surveillance (e.g. nationality, presence in a given place, health status…). This surveillance may enable the identification of one or several members of this group or to the application of a decision to one or several person, within this group, by technology. *"Mass surveillance technologies"* are technologies that enable mass surveillance, by themselves or through combination of several technologies and techniques. Finally, surveillance is biometric where it includes the use of biometric identifiers, including behavioural and psychological characteristics, in order to detect, classify or identify individuals. Surveillance is deemed to be behavioural where it is based on behavioural, psychological, or emotional signals. Biometric or specifically behavioural criteria may be used at any stage of the application of the surveillance technologies.

Biometric and behavioural mass surveillance technologies include non-exhaustively the establishment of databases of directly or indirectly nominative biometric or behavioural information as well as video, audio and other behaviour detection technologies that enable the identification or detection of individuals based on biometric or behavioural criteria. Audio and video surveillance will be included in the study where they are not used in association with behavioural or biometric criteria but are likely to enable the application of biometric and behavioural recognition techniques in a second phase. Other surveillance techniques and databases will also be included insofar they might feed a biometric mass surveillance system.

2.4 METHODOLOGY

The current report is primarily based on desk research and on remote interviews of specialists who are mentioned in related footnotes.

The assessment of the impacts of the use of biometric and behavioural mass surveillance technologies on fundamental rights is proposed under section 5 of the current report. This was carried out through a state-of-the-art Privacy Impact Assessment (PIA)[97]. A PIA, like a Data Protection Impact Assessment (DPIA), consists of assessing the impact of an initiative or a technology on a series of fundamental rights and freedoms.[98]

The retained PIA method[99] was applied to findings mentioned in the other sections of the current report in relation to the context of biometric mass surveillance (sections 3, 4.2, 4.3 and 7 of the current study) and in relation to the fundamental rights that are at stake (subsection 4.1.2 of the current report). This has been done taking into account the description of technology[100]. We assessed the impacts on fundamental rights in two stages. Firstly, we assessed the compliance of laws and practices with the conditions under which fundamental rights can be limited. These conditions are described in subsection 4.1 of the current study. Indeed, a failure to respect these conditions (i.e. necessity and proportionality requirements) already constitutes an impact per se on the fundamental rights at stake, because it basically constitutes a violation of these rights. In a second phase, we focussed on the identification and assessment of the impacts that laws and practices might indirectly cause to the fundamental rights at stake[101] – such impacts being likely to go undetected during a necessity and proportionality analysis.

1. Thomas More, Libellus vere aureus nec minus salutaris quam festivus de optimo reip. statu, deque nova Insula Utopia, Louvain, Thierry Martens, 1516. In relation to the different versions of this book, see Jean-François Vallée, 'Le livre utopique', in Mémoires du livre / Studies in Book Culture, Vol. 4, n° 2, Spring 2013, https://doi.org/10.7202/1016737ar.

2. Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 16.

3. Marie-Claire Phélippeau, 'Controversial More and Puzzling Utopia: Five Hundred Years of History', in Utopian Studies, Vol. 27, n°3, Special Issue: On the Commemoration of the Five Hundredth Anniversary of Thomas More's Utopia—Part II, 2016, p. 569-585, Penn State University Press, https://doi.org/10.5325/utopianstudies.27.3.0569 ; Philippe Godding, 'Thomas More, de procès en procès', in Bulletin de la Classe des lettres et des sciences morales et politiques, tome 13, n°1-6, 2002, p. 73-88, https://doi.org/10.3406/barb.2002.23487; Robert M. Adams, 'Preface', in Thomas More, Utopia, Norton Critical ed., W. W. Norton & Co, 3rd ed., 2011.

4. Michael J. Griffin and Tom Moylan, Exploring the Utopian impulse: Essays on utopian thought and practice, Peter Lang AG, International Academic Publishers, Bern 2007, especially p. 52 and p. 279 where the authors refer to Ernst Bloch (Das Prinzip Hoffnung, Vol. 3, Franfurt: Suhrkamp, 1985).

5. See for example Charles-François Tiphaigne De La Roche, Giphantia, or A view of what has passed, what is now passing, and, during the present century, what will pass, in the world, London, Printed for R. Horsfield, 1761, translated from the original French published in 1740, available at https://archive.org/details/giphantiaorviewo00tiph/page/n5/mode/2up; Franz Kafka, Das Urteil (The Trial), 2012, published in 1913 in Max Brod, Kurt Wolff (ed.): Arkadia, Ein Jahrbuch für Dichtkunst, Leipzig ; Georges Orwell, 1984, Secker & Warburg, London, 1949 (on the two latter books, see David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 144); Alain Damasio, La zone du dehors, Gallimard, 2021.

6. Alexis de Tocqueville, Democracy in America, translated by Henry Reeve, Saunders and Otley, London, 1835, Part II, Book IV, Chapter VI: "the species of oppression by which democratic nations are menaced is unlike anything that ever before existed in the world […] The first thing that strikes the observation is an innumerable multitude of men, all equal and alike, incessantly endeavouring to procure the petty and paltry pleasures with which they glut their lives. […] Above this race of men stands an immense and tutelary power, which takes upon itself alone to secure their gratifications and to watch over their fate. That power is absolute, minute, regular, provident, and mild. It would be like the authority of a parent if, like that authority, its object was to prepare men for manhood; but it seeks, on the contrary, to keep them in perpetual childhood: it is well content that the people should rejoice, provided they think of nothing but rejoicing. For their happiness such a government willingly labours, but it chooses to be the sole agent and the only arbiter of that happiness; it provides for their security, foresees and supplies their necessities, facilitates their pleasures, manages their principal concerns, directs their industry, regulates the descent of property, and subdivides their inheritances: what remains, but to spare them all the care of thinking and all the trouble of living?". See also Etienne de la Boétie, Discourse on voluntary servitude, 1576.

7. Albrecht Funk, John Torpey: The invention of the passport. Surveillance, Citizenship and the State, Crime, History and Societies, Varia, Vol. 5, n°2 - 2001, p. 157-158, n°1, also available at https://doi.org/10.4000/chs.745. The author quotes Gerard Noirel (Immigration, citizenship and national identity, 1988).

8. Albrecht Funk, John Torpey: The invention of the passport. Surveillance, Citizenship and the State, already mentioned, n° 3. The author refers to John Torpey, The invention of passport : Surveillance, Citizenship and the State, Cambridge University Press, New York, 2000, available at https://archive.org/details/pdfy-S0NQwPjPkMlzZ2eS/mode/2up?view=theater.

9. John Torpey, The invention of the passport : Surveillance, Citizenship and the State, Cambridge University Press, New York 2000, p. 24, available at https://archive.org/details/pdfy-S0NQwPjPkMlzZ2eS/mode/2up?view=theater. See also Gérard Noirel, Surveiller les déplacements ou identifier les personnes ? Contribution à l'histoire du passeport en France de la 1ère à la 3ème République, Génèses, vol. 30, 1998, p. 78, also available at https://www.persee.fr/doc/genes_1155-3219_1998_num_30_1_1497.

10. John Torpey, The invention of the passport: Surveillance, Citizenship and the State, already mentioned, p. 24.

11. Translated from French. Vincent Milliot, 'L'écriture du chaos. Les « mémoires » de Jean-Charles-Pierre Lenoir (1732-1807) ou le monde perdu d'un ancien lieutenant général de police', in Annales historiques de la Révolution française 2013/3, n° 373, p.35-57, also available at https://www.cairn.info/revue-annales-historiques-de-la-revolution-francaise-2013-3-page-35.htm.

12. Translated from French. Vincent Milliot, already mentioned, footnote n°24.

13. Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 16.

14. Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 21.

15. Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 24.

16. Albrecht Funk, 'John Torpey : The invention of the passport. Surveillance, Citizenship and the State', in Crime, History and Societies, Varia, Vol. 5, n°2 - 2001, p. 157-158, n° 4, also

available at https://doi.org/10.4000/chs.745.

17. *Vincent Denis, 'Identifier par le corps avant la biométrie aux XIVe - XIXe siècles', already mentioned, p.31.*

18. *Translated from French: Vincent Denis, 'Identifier par le corps avant la biométrie aux XIVe - XIXe siècles, in Ayse Ceyhan and Pierre Piazza, L'identification biométrique : Champs, acteurs, enjeux et controverses, Editions de la Maison des Sciences de l'Homme, 2011, p. 25-37, p. 29 and p. 35.*

19. *Translated from French: Gérard Noirel, Surveiller les déplacements ou identifier les personnes ? Contribution à l'histoire du passeport en France de la 1ère à la 3ème République, Génèses, vol. 30, 1998, p. 100.*

20. *It appears that even during the French revolution, there still were multiple endeavours "to issue passports and identification papers that tried [to keep] the movements of those who were perceived as enemies of the revolution, under surveillance, (aristocratic émigrés, insurrectionists of the Vendée, foreigners)": Albrecht Funk, John Torpey: The invention of the passport. Surveillance, Citizenship and the State, already mentioned, n° 2. In the same line, in 2019, the lawyer François Sureau expressed indignation at the power granted to the French State to control "the participation of each individual in a protest" and therefore to "choose its opponents": François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 20.*

21. *See subsection 4.1 of the current study.*

22. *Cesare Beccaria, Des délits et des peines, Preface by Robert Badinter, translated by Maurice Chevallier, ed. Flammarion, 1991, p. 20 and 169.*

23. *Cesare Beccaria, Des délits et des peines, already mentioned, p. 72.*

24. *Cesare Beccaria, Des délits et des peines, already mentioned, p. 166.*

25. *Gérard Noirel, already mentioned, p. 99.*

26. *Ilsen About, 'Classer le corps : l'anthropométrie judiciaire et ses alternatives, 1880-1939', in Ayse Ceyhan and Pierre Piazza, L'identification biométrique : Champs, acteurs, enjeux et controverses, Editions de la Maison des Sciences de l'Homme, 2011, p.39-61, p. 43. See also Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 102.*

27. *Ilsen About, 'Classer le corps : l'anthropométrie judiciaire et ses alternatives, 1880-1939' already mentioned, p. 44-45.*

28. *Ilsen About, 'Classer le corps : l'anthropométrie judiciaire et ses alternatives, 1880-1939', already mentioned, p. 48-49.*

29. *Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 42; Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, already mentioned, p. 103.*

30. *Pierre Piazza, 'Bertillonage: the International circulation of practices and technologies of a system of forensic identification', translation by Patrica Bass of the French version entitled 'Identification, contrôle et surveillance des personnes', Revue Hypermedia – Histoire de la justice, des crimes et des peines, n° 3, https://journals.openedition.org/criminocorpus/2970.*

31. *Pierre Piazza, 'Bertillonage: the international circulation of practices and technologies of a system of forensic identification', already mentioned, n°3.*

32. *Ilsen About, 'Classer le corps : l'anthropométrie judiciaire et ses alternatives, 1880-1939', in Ayse Ceyhan and Pierre Piazza, L'identification biométrique : Champs, acteurs, enjeux et controverses, Editions de la Maison des Sciences de l'Homme, 2011, p.39-61, p. 43. See also Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 52 s.*

33. *John Torpey, The invention of the passport : Surveillance, Citizenship and the State, Cambridge University Press, New York 2000, p. 93, available at https://archive.org/details/pdfy-S0NQwPjPkMlzZ2eS/mode/2up?view=theater.*

34. *John Torpey, The invention of the passport : Surveillance, Citizenship and the State, already mentioned, p. 93-110.*

35. *John Torpey, The invention of the passport : Surveillance, Citizenship and the State, already mentioned, p. 111.*

36. *John Torpey, The invention of the passport : Surveillance, Citizenship and the State, already mentioned, p. 112-115.*

37. *John Torpey, The invention of the passport : Surveillance, Citizenship and the State, already mentioned, p. 116-133.*

38. *Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p. 44-45.*

39. *David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 32.*

40. *John Torpey, The invention of the passport : Surveillance, Citizenship and the State, already mentioned, p. 123.*

41. *David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 32.*

42. *Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p. 44-45.*

43. *David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 32.*

44. *David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 27, 32, 38.*

45. *David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 76. See also 'Identity cards abolished after 12 years - archive, 1952', The Guardians, https://www.theguardian.com/politics/2018/feb/22/identity-id-cards-abolished-1952.*

46. *Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 3-8; David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 5 and p. 79, referring to David Cameron.*

47. *Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 45.*

48. *David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 49.*

49. *David Lyon, Surveillance Studies: An*

Overview, ed. Polity, 2007, p. 49.

50. *See subsection 4.1.1 of the current study.*

51. *Robert Badinter, 'Preface', in Cesare Beccaria, Des délits et des peines, translated by Maurice Chevallier, ed. Flammarion, 1991, p. 9-47, p.47, see also p. 39.*

52. *See subsection 4.1.3 of the current study.*

53. *Georges Langrod, 'Le traitement électronique des données et la recherche de protection contre leur utilisation abusive (modèle Allemand du Land de Hesse)', in La Revue Administrative, 1971, p. 692-695, 27 April 2012, also available at https://www.bijus.eu/?bijusbiblio_deutsch=landesdatenschutzgesetz-vom-07-10-1970-hessen.*

54. *Sweden, Data Protection Act (No. 289 of 1973), https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=55767.*

55. *The United Kingdom, Data Protection Act 1984, https://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf.*

56. *Graham Greenleaf, 'Countries with Data Privacy Laws – By Year 1973-2019', 10 May 2019, p. 1, available at SSRN: https://ssrn.com/abstract=3386510 or http://dx.doi.org/10.2139/ssrn.3386510; Priscilla M. Regan, 'Global privacy issues', 1 March 2010, https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-205?rskey=X0Y2jK; in relation to France, see Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p. 46; French Sénat, Service des Affaires européennes, 'La protection des données personnelles, note de synthèse', October 1999, https://www.senat.fr/lc/lc62/lc62.html.*

57. *Council of Europe, Convention 108 and Protocols, https://www.coe.int/en/web/data-protection/convention108-and-protocol.*

58. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 1§1, Official Journal L 281, 23/11/1995, p. 0031- 0050, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.*

59. *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), OJ L 119, 4.5.2016, p. 1–88, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679.*

60. *Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 8.*

61. *Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 9.*

62. *Olivier Aïm, Les théories de la surveillance, Du panoptique aux Surveillance Studies, Armand Colin, 2020, p. 104; Simon A. Cole, 'La saisie de l'ADN aux Etats-Unis et au Royaume-Uni à des fins d'identification des individus : origines et enjeux', in Ayse Ceyhan and Pierre Piazza, L'identification biométrique : Champs, acteurs, enjeux et controverses, Editions de la Maison des Sciences de l'Homme, 2011, p. 63-78, p. 65 s.*

63. *Olivier Aïm, Les théories de la Surveillance – Du panoptique aux Surveillance Studies, ed. Armand Colin, 2020, p. 104.*

64. *David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p.4; Shoshana Zuboff, The age of surveillance capitalism: The fight for a human future at the new frontier of power, ed. Profile Book, 2019, introduction.*

65. *Olivier Tesquet, État d'urgence technologique, 2021, p. 12; François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 6; Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 3-8; David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 177.*

66. *Estelle De Marco, 'La captation des données' (Data capture), in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux, Institut Universitaire Varenne, coll. colloques et essais, 4ème trim. 2017, pp. 91-107 ; Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p. 45-52.*

67. *Bernard Didier and Carole Pellegrino, 'Les technologies identitaires biométriques : que fait l'Europe face aux États-Unis ?', in Ayse Ceyhan and Pierre Piazza, L'identification biométrique : Champs, acteurs, enjeux et controverses, Éditions de la Maison des Sciences de l'Homme, 2011, p. 101-110, p.101 s.; Olivier Tesquet, Etat d'urgence technologique, Premier Parallèle, 2021, p. 9 s.*

68. *Pierre Piazza and Ayse Ceyhan, 'Introduction', in Ayse Ceyhan and Pierre Piazza, L'identification biométrique : Champs, acteurs, enjeux et controversies, already mentioned, p.14.*

69. *David Lyon, Surveillance Studies: An overview, ed. Polity, 2007, p. 12 and p. 155.*

70. *Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 79; David Lyon, Surveillance Studies: An overview already mentioned, p.115, 161 s, 171 s, 185, 191-192; Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p. 55.*

71. *Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p. 51-56.*

72. *Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p. 18, 52; David Lyon, Surveillance Studies: An overview, already mentioned, p. 191-192.*

73. *See subsections 3.2, 4 and 5 of the current study.*

74. *Louis Favoreu, 'Universalité des droits fondamentaux et diversité culturelle', in L'effectivité des droits fondamentaux dans les pays de la communauté francophone, colloque international de l'île Maurice, 29 Sept.-1 Oct. 1993, AUPELF/UREF1994, p. 48, referred to in François Terré, Introduction générale au droit, Précis Dalloz, 6th ed., 2003, p. 7; Serge Guinchard, 'Le procès équitable : droit fondamental ?', AJDA special 20 July – 20 August 1998, p. 191.*

75. *Claude-Albert Colliard, Libertés*

publiques, Dalloz, 6th ed., 1982, p. 23.

76. Translated from French: Louis Favoreu et al., Droit des libertés fondamentales, Dalloz, 3rd ed., 2005, n° 57.

77. The two quotations in this sentence are issued from Gérard Cornu, Association Henri Capitant, Vocabulaire juridique, 7th ed., Quadrige/PUF, June 2005, p. 330 (translated from French).

78. This definition, proposed by Tom Bigham, is considered by the Venice Commission of the Council of Europe as the definition that "covers most appropriately the essential elements of the rule of law": Council of Europe, European Commission for democracy through Law (Venice Commission), Report on the rule of law, Adopted by the Venice Commission at its 86th plenary session, 25-26 March 2011, n° 36, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e.

79. Council of Europe, European Commission for democracy through Law (Venice Commission), Report on the rule of law, v, n° 41 s.; Council of Europe, European Commission for democracy through Law (Venice Commission), Rule of law Checklist, adopted by the Venice Commission at its 106th Plenary Session, 11-12 March 2016, CDL-AD(2016)007-e, n° 18, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)007-e.

80. Council of Europe, European Commission for democracy through Law (Venice Commission), Rule of law Checklist, v, n° 24.

81. Council of Europe, European Commission for democracy through Law (Venice Commission), Rule of law Checklist, already mentioned, n° 15 and 16.

82. Suggested translation by David Lyon, Surveillance Studies: An overview, ed. Polity, 2007, p. 14.

83. David Lyon refers to a "focused, systematic and routine attention to personal details": Surveillance Studies: An overview, already mentioned, p. 14.

84. Le Petit Robert, dictionnaire de la langue française, 2000, definitions of "surveillance" (surveillance) and "surveiller" (to watch over), p. 2445-2246.

85. David Lyon, already mentioned, p. 14 and p. 159.

86. This notion is rarely defined outside specific contexts (alternative to imprisonment, medical care). The dictionary Le Petit Robert defines "electronic surveillance", in the context of medical care, as an "electronic equipment that records all important functions of a patient" (dictionary already mentioned). As a result, the scope of the control that is exercised depends on the specific purposes of the surveillance mechanism in place.

87. The notion of group implies that the link between concerned people goes beyond the specific purposes of surveillance. In relation to the reference to an entire or significant part of the population, to base the definition, see US Legal, https://definitions.uslegal.com/m/mass-surveillance/; Benson Egwuonwu, 'What Is Mass Surveillance And What Does It Have To Do With Human Rights?', 11 April 2016, https://eachother.org.uk/explainer-mass-surveillance-human-rights/.

88. See Ayse Ceyhan, 'Editorial. Identifier et surveiller : les technologies de sécurité', in Culture et Conflits n°64 – Hivers 2006, 1, https://journals.openedition.org/conflits/2138, (translated from French): "Identification and surveillance – which were a priori seen as two separate activities – are now very much linked, even considered to be the same, and this assimilation gradually increased with the adoption of security technologies, which are being presented as a highly scientific mechanism to combat current and future risks and dangers. Within that framework, identifying means not only to assign a recognisable identity to an individual by means of relatively stable criteria, but it also means to be able to recognise this individual's movements, actions, relationships, preferences and even their plans. In parallel, surveillance is not anymore reduced to the tracing of an individual, but it also implies the capability to identify the latter with certainty, based on their habits, behaviours and mobility. This confusion is generated by the deployment of sophisticated security technology that proceed with the identification and with the surveillance of an individual based on the examination of their innate and unchangeable characteristics, what is know as 'bios'".

89. Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, August 2021, p. 8 and 14, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

90. Christiane Wendehorst and Yannic Duller, already mentioned, p. 34.

91. Christiane Wendehorst and Yannic Duller, already mentioned, p. 8; Francesco Ragazzi et al., Biometric mass surveilllance, Part I, Chapter 2.

92. Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, already mentioned, p. 8.

93. Christiane Wendehorst and Yannic Duller, already mentioned, p. 14.

94. Christiane Wendehorst and Yannic Duller, already mentioned, p. 8.

95. See for example Tim Van hamme et al., 'Improving Resilience of Behaviometric Based Continuous Authentication with Multiple Accelerometers', in Livraga G., Zhu S. (eds), Data and Applications Security and Privacy XXXI, DBSec 2017, Lecture Notes in Computer Science, Vol. 10359, Springer, Cham, https://doi.org/10.1007/978-3-319-61176-1_26.

96. In relation to this sentence and the previous one, see Christiane Wendehorst and Yannic Duller, already mentioned, p. 8.

97. In relation to the notion of PIA, see Estelle De Marco, Deliverable D2.4a - Privact Impact Assessment of the MANDOLA outcomes, July 2017, MANDOLA EU project, GA n° JUST/2014/RRAC/AG/HATE/6652, subsection 3.1., http://mandola-project.eu/m/filer_public/97/af/97af7af5-9145-4564-8cb6-fb3f363d3d92/mandola_d24a.pdf.

98. Estelle De Marco, 'A DPIA is a PIA: consequences in terms of implementation and scope', March 2019, publication written within the framework of the INFORM EU project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-

AG-2016, GA n° 763866, https://www.inthemis.fr/ressources/A-DPIA-is-a-PIA.html. See also the French Data Protection Authority (CNIL) guidelines to perform a DPIA, https://www.cnil.fr/en/guidelines-dpia.

99. Estelle De Marco, Deliverable D2.4a - Privact Impact Assessment of the MANDOLA outcomes, already mentioned, subsection 4.3.3.1. The state of the art has been adapted to the context and particularities of the current study.

100. Francesco Ragazzi et al., Biometric & behavioural mass surveillance in the EU Member states, October 2021, http://extranet.greens-efa.eu/public/media/file/1/7297; Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, August 2021, section 1, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

101. These fundamental rights (listed under the subsection 4.1.2 of the current study) are the "values" submitted to the impact analysis, which includes the risk analysis. In a traditional risk analysis, these "values" are sometimes called "primary assets" (see for example the EBIOS method for assessing and treating digital risks, https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/; see also the norm ISO/IEC 27005).

3

CONTOURS AND CONTEXT OF THE USE OF SURVEILLANCE TECHNOLOGIES

3.1 CURRENT USE OF MASS SURVEILLANCE TECHNOLOGIES WITHIN THE EU & WESTERN BALKANS

3.1.1 USE, BY PUBLIC AUTHORITIES, OF BIOMETRIC MASS SURVEILLANCE TECHNOLOGIES

EUROPEAN UNION BORDER MANAGEMENT

At the level of the European Union, border management policies successively introduced and imposed the implementation of biometrics in visas[102], passports[103], and identity cards[104]. 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[105]. Nowadays, the information systems that support these policies gather more than 53 million pieced of biometric data[106]. These systems, managed by eu-LISA[107], are the VIS[108], the SIS I a II[109], the Eurodac[110], the ECRIS[111], the ETIAS[112] and the Entry/Exit System (EES), which *"will electronically register the name, type of travel document, biometrics (4 fingers and face), and the date and place of entry and exit of third-country nationals visiting the Schengen area for a short stay"*[113].

Providers of hardware used to operate the VIS, the SIS, and the Eurodac systems, as well as the Europol own database, are Hewlett Packard and Dell. Providers of softwares are American and European[114]. In addition, these systems use an Automated Fingerprint Identification System (AFIS), which is expected to include *"facial recognition as a major component"*[115] in the future and *"to serve as a basis for the development of a shared Biometric Matching Service storing biometric templates"*[116] as suggested in the proposal for interoperability between EU information systems[117]. This interoperability was established by two regulations in 2019118, thus giving rise to a *"vast biometric database covering* 28 *countries"*[119] to which security and law enforcement have access in the pursuit of purposes that are further extended[120].

CITIZENS IDENTIFICATION IN EU MEMBER STATES

In relation to biometric identity cards specifically, all the member states of the European Union had the obligation to implement this new format on 5 August 2021. An important number of them did it that very day[121].

Even though the EU Regulation on strengthening the security of identity cards imposes the suppression of biometric data once identity cards have been issued[122], unless another *"necessary and proportionate"* processing is established nationally *"in accordance with Union and national law"*[123], it appears that some EU member states have seized this opportunity to collect such data for national purposes[124].

In addition, numerous countries allocate their nationals a unique national Code[125], or use to this end a sectoral number[126], such unique identifier being directly linked, in some countries, to biometric identity cards[127]. It is important to observe that assigning to each national a unique identification number makes it very easy to interconnect databases, in a context where serious temptations of interconnecting administrative files are noticed[128]. The major difference between a biometric identifier and a unique national number is that the former

makes it possible to refer to a natural person with certainty. In addition, a biometric identifier cannot be revoked or modified, even in case of theft. Such an identifier is therefore particularly dangerous to the safety of individuals.

VIDEO-SURVEILLANCE IN EU MEMBER STATES

EU member states also increasingly use video-surveillance. Even though China *"leads the world"* in that area, with *"54% of the world's* 770 *million surveillance cameras"*[129], an author observed in 2010 that across the European continent, CCTV systems were *"installed in towns and cities […], with the result that public area surveillance is an inescapable fact of life for a growing number of Europeans"*.[130] The current precise number of cameras deployed is unknown, because their implementation depends on different categories of stakeholders without any reporting system being established[131]. However, available figures show that London held the lead when the UK was part of the European Union, with more than 691,[000] cameras and a ratio of 73.31 cameras for 1,000 inhabitants[132]. According to the same study[133], Berlin in Germany commands 223,000 cameras for a ratio of 6.25 cameras for 1,000 inhabitants, Madrid in Spain commands 34,000 cameras for a ratio of 5.1 cameras for 1,000 inhabitants, Paris in France commands 42,500 cameras for a ratio of 3.84 cameras for 1,000 inhabitants and Athens in Greece commands 10,800 cameras for a ratio of 3.44 cameras for 1,000 inhabitants.

These systems of surveillance use cameras and do not necessarily include innovative features such as facial recognition. However, *"possibilities for continuous improvement of these devices remain wide as well as their areas of application"*[134]. This is confirmed by the weight of the industry[135] and the series of experiments that have been co-funded for several years by the European Union[136]. In addition, a study shows that *"since 2010, a revolution has begun in video analytics. Thanks to Convolutional Neural Networks, Deep Learning techniques, [and] object recognition, image segmentation and labelling [have proved] impressively efficient, up to the point where the machine, using a software built on top of GoogLeNet137 has demonstrated in 2015 an ability to identify objects in still images that is almost identical to humans […]. In 2015, the Chinese company BAIDU also claimed actual superiority of machine image"*[138].

In addition, numerous cases of biometric surveillance are reported. For example, in July 2021, a report revealed an *"increasing trend of implementation of […] biometric surveillance measures across numerous localities throughout Germany"* and the use, by *"municipalities and police forces in the Netherlands [of] facial recognition technology and other forms of biometric surveillance in a multitude of ways"*[139]. Facial recognition is also widely used in the United Kingdom[140]. It is also progressively expanding in France[141], in Romania[142], and globally in all EU member states[143] and states of Western Balkans[144].

Moreover, several current and former EU member states initiated the deployment of body-worn cameras for law enforcement. It is the case in France, the United Kingdom, Romania,[145] Italy[146] and Greece[147]. In some countries, other stakeholders such as border police[148] or ambulance services[149] are also equipped with body-worn cameras. Amongst camera models used, the American company Motorola VB400[150] enables the sending of live images that can technically be monitored using biometric or behavioural recognition systems, directly or in a second phase[151]. Currently, such use is prohibited in some countries, such as in Italy, following a decision by the Data Supervisory Authority[152]. The main objectives announced for the use of body-worn cameras are safety improvement for the police and the public, police accountability enhancement, and evidence production before a court.[153]

The use of mobile technologies has particularly been noticed during the covid-[19] pandemic. While Singapore experimented with autonomous robots in order *"to detect bad behaviour such as flouting of COVID-19 safety measures, smoking in prohibited areas and the improper parking of bicycles"*[154], Italy, the United Kingdom, and France used drones in order to monitor compliance with health measures[155], a decision later disapproved in the latter State by the French Data Protection Authority, in January 2021[156].

EXPERIMENTS

Finally, several projects were conducted or are still ongoing under the responsibility or with the cooperation of local authorities or public companies, in addition to participation to EU co-funded research projects[157]. For example, in 2013, a system named AVATAR, designed to analyse *"nonverbal and verbal behaviour"* of travellers during interviews, was experimented in the Bucharest

airport.[158] As of February 2020, a series of law enforcement and government-affiliated agencies used, without managerial oversight and outside any legal framework, software aiming to perform facial recognition based on photographs collected on social networks by Clearview AI, which was the provider of this solution[159]. In 2019, the French city of Nice utilised facial recognition during the carnival, with a view to detecting persons already registered in a database, with the consent of persons involved.[160] During the same year, the same city also envisioned experimenting with a system capable of detecting travellers' emotions in public transportation, with the aim of identifying potential suspects before an incident occurs[161]. This project was abandoned due to a technical issue.[162]

TECHNOLOGY PROVIDERS

Globally, the large number of CCTV and biometric technology providers[163] is noteworthy, with a prevalence in Europe of certain companies such as THALES, IDEMIA[164], SAFRAN and EADS[165]. Public authorities also tend to contract with enterprises that offer them innovative solutions[166]. It seems that the most commonly used system is technology delivery, with or without assistance for analysis. That being said, two authors observed in 2011 that the biometric market remains opaque for several reasons: the scarcity of supporting studies; andthe opacity organised by operators themselves, in order to establish high prices of access to information. In addition, the security sector is partly subjected to defence secrecy classification.[167]

3.1.2 OTHER USAGES OF SURVEILLANCE TECHNOLOGIES

Other practices that result in the monitoring or collection of personal data are in use, both offline and online. Reference to these practices is important because the resulting databases are often accessible to law enforcement and government agencies, in particular for the purposes of internal security and the prevention and repression of crime. Such access is supposed to be provided for by law[168] but it sometimes occurs outside any legal framework[169]. This access may increase the impact of the use of biometric surveillance technology, by supplying it either with information that enables the technology to operate, or with additional information relating to the persons identified.

The public and private sectors increasingly propose authentication functions based on biometric recognition, which allows some stakeholders to foresee that the *"global facial recognition market will experience 12.4 percent compound annual growth […] from 2021 to 2025"*[170]. Several EU member states, such as France[171], are progressively implementing biometric identifications techniques in order to enable access to public services, while other EU member states are exploring the possibility to develop them[172].

As regards the private sector, 62% of enterprises declared in 2018 that they were using biometric authentication techniques and 24% declared they were considering using such technologies within two years[173]. Several banks, for instance, recently began to invite their clients to opt-in for a biometric credit card[174] while Genesis, a Hyundai Motor brand, announced that face and finger recognition will be proposed on its electric sport utility vehicle in order to replace keys and to activate some features[175]. In addition, numerous computing devices enable login based on biometric identification techniques[176]. The academic sector also uses such technologies. For example, in the United Kingdom, fingerprints were used in order to handle absenteeism, to charge meals, and as a substitute for library cards, before legislation imposed a need for parental consent[177]. In France, authentication functions based on hand contour recognition are used in order to frame access to school canteens[178].

Both the private and the academic sectors also use surveillance techniques based on biometric or behavioural criteria, for example enterprises such as supermarkets, which use such technology in order to detect fraudulent activity[179]. Some employers show an interest in the use of continuous recognition systems, based inter alia on user keystroke, in particular since the Covid-19 pandemic, which led to a massive increase in remote work[180]. During the successive lockdowns due to the pandemic, some educational institutions also imposed invigilation software in order to monitor exams[181]. Some works relating to smart advertising boards were also reported[182],

In addition, some Internet service providers propose functions that imply the processing of biometric or behavioural information. These features include for example the possibility to exchange through video conference using personal computers' webcams[183]. These features may alternatively only rely on voice, and enable its supporting software to answer a user's vocal instruction[184]. Lastly, Amazon unveiled its first *"house assistant robot"*, which can *"map a house and answer vocal queries in order to videotape one room or another"*, recognise faces, learn the family members' habits and *"remind"* each of these members *"of their tasks"*, in addition to enabling videoconference.[185]

Moreover, smart meters are progressively implemented in Europe[186], whereas numerous applications, especially on smartphones and watches, propose features such as the possibility to justify one's vaccination status[187], assess sporting efforts[188], and to monitor vital functions[189]. These applications generally collect various other types of information on their users[190]. Numerous mobile devices such as smartphones, tablet PCs and smartwatches also include accelerometers, which are *"sensors for measuring acceleration force"* commonly used for *"automatic image stabilisation, device orientation detection, and shake detection"*[191]. Data produced by accelerometers is generally accessible to other applications, because such data is *"widely regarded as not privacy-intrusive"*. However, it has been demonstrated that accelerometers can, conversely, *"infer highly sensitive information about people"* including their identification *"based on biometric movement patterns"*.[192] These considerations must be read in conjunction with a study that reveals that smartphone users touch their devices on average 2617 times a day[193].

In relation to online activities, it can be noticed that internet users are invited to store their personal data on private clouds whose security is not always ensured with certainty, including from the cloud provider[194]. This particularly applies to providers that propose to concentrate, in a single place, a lot of very sensitive information such as energy, telephone and Internet access provider invoices, health insurance cards, pay sheet, tax notices, and bank statements[195]. The vast majority - if not all - of such providers fetch documents directly from their original or official sources, which means that even with strong end-to-end encryption[196], these providers may have access to the real content at some point and overall security is only based on ethics and public statements, and cannot be directly enforced or verified by users. As a result, any mind shift, business plan, company acquisition or disproportionate request from intelligence services[197] may lead to disproportionate access to users' information, which is all the more problematic, in relation to the preservation of private life, as stored information is sensitive.

Finally, it is to be noted that all Internet service providers retain certain traces of Internet use, to a greater or lesser extent depending on their precise activities and the legal obligations that apply to these activities[198], whereas the advertising and service industries collect various information relating to internet users in order to set their profile[199]. Recourse to data engineering has also been alleged to be a governmental practice, at least in the USA, in order to automatically detect and predict the behaviours of enemies and rebels and distinguish them from the rest of the civilians[200].

3.2 THE ROLE OF EUROPEAN AND NATIONAL ACTORS IN THE FIELD

THE ROLE OF THE EUROPEAN UNION

Previous analysis shows that the European Union *"has undoubtedly played – and still plays – a central role in the field of security technology, becoming a real 'motor' for its member states, particularly with regards to biometrics"*[201]. The European Union accompanied the adoption of security technology with a *"legal framework"* that it claims to be *"coherent"*.[202] However, the lawyer Sylvia Preuss-Laussinotte believes that this notion of *"coherence"*

actually tends to support the *"technical convergence of European systems that contain biometric data"*, including for budgetary reasons, and that it partly aims to favour *"interconnections between national and European databases, especially biometric"*[203].

This EU policy expands to the Western Balkans, through the support of the European Commission to bring to that region *"the benefits of the digital transformation"*[204], supporting in particular the *"strengthening of Balkan countries capabilities in terms of data collection and exchange"*[205]. The Council, for its part, *"underscored its intention to support the Western Balkan states in the development of interoperable systems for the biometric registration of asylum applicants and irregular migrants […] thereby rendering it compatible with EU systems"*[206].

THE ROLE OF THE UNITED STATES OF AMERICA

Several authors explain that the above policy is the European Union's response to *"irrevocable pressure from the USA"*[207], which has been explicit *"since 11 September 2001"*[208], to make the recourse to biometry a priority objective *"in the name of the struggle against terrorism"*[209]. Edgar A. Whitley and Gus Hosein highlight that, in order to answer that demand, the Council of the European Union pressured the European Parliament to prevent a refusal *"to include mandatory fingerprinting for all EU citizens in the draft regulation"* that standardises EU passports[210]. E. A. Whitley and G. Hosein question *"the legality of this course of action"*, especially because *"the inclusion of fingerprints in the EU passports system [was not] a requirement from the U.S. authorities"*.[211] They observe that Australia, Canada, and the U.S. rejected implementing additional biometrics in their own passports, other than a *"tamper-proof image of the face"*.[212] They clarify that US requirements were to implement machine-readable passports that include *"only a digital photograph on a chip in the passport"*[213]. They report that the Chairman of the US Congressional committee responsible for the biometric passport deadline, himself, regretted the EU choices, declaring that *"much expense and public consternation could have been avoided by a less technically ambitious approach, one that simply met the terms of the Act as written"*[214].

ORGANISED SHORT-CIRCUIT OF DEBATES AT THE EUROPEAN AND NATIONAL LEVELS

According to Whitley and Hosein, the EU approach therefore only *"serves an EU-domestic policy to generate a registry of fingerprints of all EU citizens and residents"*[215], a statement which could be extended to facial images. They warn about the tendency of governments *"to short-circuit debate and deliberation"*, in particular on identity policy, which is not for them a surprise because where substantive debate took place in the past, *"limitations were often placed on the government's vision […] whether to limit its budget, application and/or effects on freedom and privacy"*.[216] The authors observe that most identity policies were rather established through minimal deliberation, *"during darker times where political debate was unlikely [or] by government diktat"*.[217]

Thisis further shown where technology risks are most of the time not seriously assessed, policies being *"never adequately reviewed at any level as each level presumes that the other level will or has done it"*.[218] In this respect, Sylvia Preuss-Laussinotte observes, referring to a statement from a representative of the company SAGEM, that the use of biometry in travelling documents *"becomes the seed of a world-wide interoperable biometry"* and that *"it is precisely in the implementation of this generalised biometric globalisation that arise the question of its fragility and the question of the security-related European policy"*.[219]

These concerns have largely not been answered, beyond rhetorical statements of commitment to fundamental rights protection. Indeed, the EU does not, actually, respond to them, while it mostly organises identity and security policy through regulations, which prevents any serious debate at national levels. Even the transposition of EU Directives leaves little room for national debates. This observation raises the issue of the intentional weakening of Parliaments through the strategic use of international influences or obligations *"to circumvent national deliberative processes"*[220]. Whitley and Hosein call this practice *"policy laundering"*.[221]

Indeed, we can especially observe that, even though the EU member states may have encountered some slowness in following the EU decisions on biometric identity cards[222], the fact remains that the EU policy was for them an opportunity to implement or to

justify such cards, in a context where, sometimes, first attempts in that sense failed at the national level, due to civil society protest[223]. As a result, any objection may now be rejected based on a reminder of international commitments[224]. This observation is reinforced by the fact that EU member states expressed in 2020, their wish for the development of an EU-wide public electronic identification system.[225]

Other methods to short-circuit debate are the adoption of decrees or emergency ordinances instead of laws[226], and the manipulation of public opinion. The latter has been particularly analysed by the public administration specialist Guillaume Gormand[227]. He shows that citizens' fears towards state surveillance created a hostile environment for video-surveillance. As a result, especially in France and in the United Kingdom[228], video-surveillance advocates strived to legitimise its use *"by addiction and habit"* of both citizens and public policy actors[229]. To this end, they first put forward favourable public opinion polls whose results were often manipulated[230]. In addition, especially under the presidency of Nicolas Sarkozy, *"an artificial atmosphere of fear"*[231] was deliberately created through *"a rise in national security discourse"* and the *"use of a particularly clever rhetoric designed to instil fear in the population and to call on citizens to choose between the cause of 'victims' and the cause of 'thugs'"*[232].

In 2008, in order to avoid accusations of *"security drift and of generalised surveillance"*[233], a *"semantic reversal"* led to the replacement of the expression *"video-surveillance"* with the expression *"video-protection"*. This was also reflected in legislation in 2009. However, as stated by French parliamentarians, *"video-surveillance does not protect. The recording of an offence does not prevent this offence from being committed"*.[234] The French Ministry of Home Affairs even created a logo with this new terminology, accompanied with a slogan stating *"security at the service of freedom"*[235].

The same phenomenon is observed in relation to biometry. A number of public representatives widely use shifts in meaning to present surveillance and biometrics in a favourable light, and thus increase its *"acceptability"* 236. For example several representatives of French institutions[237]. This is also the case within the institutions of the European Union[238], which present the recourse to biometry as a pledge of security, the latter being asserted as a natural need that is beyond discussion in its principle[239] and which is inherent to freedoms[240] where it does not supersede them[241]. These statements, which mostly invoke freedoms protection grounds[242] as a justification for surveillance, actually trample on fundamental principles that underpin the European legal system, in which security is conversely an exception to freedom and can only be implemented under strict conditions[243].

Citizens, deceived in relation to the efficiency and the purpose of biometric technology, are therefore deprived of real debate on these topics. Yet, such a debate is of utmost importance. Indeed, security issues affecting intimate data that cannot be revoked[244] as well as the question of whether the security brought by surveillance including biometry is real, in the face of terrorist threat[245], are as important as the challenges that are at stake in terms of choice of the societal model currently followed[246].

EU FUNDING OF A RESEARCH THAT IS CRITICISED FOR NOT BEING ETHICAL

Regardless of this - and of the fact that, as previously mentioned, some authors suggest that security public policy is partly dictated by the surveillance industry[247], at least originally - the European Union sustains innovation by funding several research projects aimed at enhancing video surveillance and biometric or behavioural identification efficiency. Some representatives of public authorities in EU member states are sometimes partners or beneficiaries of such projects[248]. These projects are criticised for failing to incorporate sufficient ethical and democratic accountability[249].

We can highlight the CHAMELEON project, which took place in 2012-[2013] and received a funding of EUR 785,[893]. It developed a video surveillance system [which] automatically combines images from multiple cameras with overlapping regions, to create a natural seamless 180 panoramic view of the monitored area [and] allows portable devices such as smart phones and tablets to stream and display the stitched video feed in real-time"[250]. *According to the Community Research and Development Information Service of the European Commission (CORDIS), this system has "*huge potential in a number of applications such as remote monitoring,

border control, temporary exhibitions and events and transport*", in addition to improving "*the working conditions of security camera supervisors".[251]

Another example is the INDECT project. With a EU contribution of almost EUR 11 million, it aimed to implement an intelligent surveillance system capable of processing all kinds of information, including mobile objects and persons as well as Internet resources including *"individual computer systems"*, with a view to detecting criminal activities and threats.[252]

Another project, the iBorderCtrl (Intelligent Portable Control System) project, which was particularly controversial[253] and renamed ICROSS[254], developed technologies *"ranging from biometric verification, automated deception detection [and] document authentication"* for automatic controls at borders[255], including a kind of *"lie detector"*[256]. The IMPULSE project, funded until January 2024, aims to perform *"a user-centric and multidisciplinary analysis on the integration of [AI and blockchain] technologies"* supporting electronic identification in EU public services.[257]

EXPORT CONTROLS

Finally, we can observe that a report from Amnesty International revealed in September 2020 that European technology companies were exporting digital surveillance technology to countries with poor human rights records[258]. At the same time, Privacy International revealed the *"EU's extensive support for surveillance in non-member countries"*[259]. As a result, the European Union *"agreed to tighten up rules for the sale and export of cybersurveillance technology"*, especially through updating *"controls of so-called dual use goods such as facial recognition technology and spyware to prevent them from being used to violate human rights"*.[260] This led to the adoption of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items (recast)[261].

However, in October 2021, a coalition of NGOs submitted a complaint to the European Ombudsman, calling on it to *«investigate evidence that several EU bodies are supporting surveillance in non-EU countries»*[262]. They argue that this support includes the provision of *«surveillance technology, training and financing»*, whereas no *«human rights risk and impact assessments»* were being carried out.[263]

3.3 CIVIL SOCIETY RESPONSES

Numerous specialists including lawyers, philosophers, sociologists, and historians[264] warn about the dangers of states' social control and biometric technology, evoking issues of opacity, security, proportionality and of a loss of meaning of the very notion of *"freedom"*[265] in a State governed by the Rule of Law.

In addition, a significant number of organisations and institutions call for a ban on biometric surveillance:

In September 2021, the United Nations High Commissioner for Human Rights published a report that notably requires imposing *"a moratorium on the use of remote biometric recognition technologies in public spaces, at least until the authorities responsible can demonstrate compliance with privacy and data protection standards and the absence of significant accuracy issues and discriminatory impacts [...]"*.[266]

In July 2021, the European Parliament adopted a resolution in which it notably called *"for the permanent prohibition of the use of automated analysis and/or recognition in publicly accessible spaces of other human features, such as gait, fingerprints, DNA, voice, and other biometric and behavioural signals"*, and to *"a moratorium on the deployment of facial recognition systems for law enforcement purposes that have the function of identification, unless strictly used for the purpose of identification of victims of crime, until"* the necessity and proportionality of such operations are ensured and demonstrated, and risks are identified and suppressed.[267]

In a joint opinion dated June 2021, the EDPB and the EDPS call inter alia, *"for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces"*[268]. Since June 2021, more than 170 NGOs have also been calling for a ban of this technology[269]. These organisations highlight that the use of biometric technology

makes it possible to *"identify, follow, single out, and track people everywhere they go, undermining our human rights and civil liberties — including the right to privacy and data protection, the right to freedom of expression, the right to free assembly and association (leading to the criminalization of protest and causing a chilling effect), and the rights to equality and non-discrimination"*. They state that these technologies, *"by design, threaten people's rights and have already caused significant harm"*. They consider that *"no technical or legal safeguards could ever fully eliminate the threat they pose"*, and for this reason they should *"never be used in public or publicly accessible spaces, either by governments or the private sector"*[270].

This initiative led to the creation of the movement *"reclaim your face"*, which gathered more than 60,[000] signatures in October 2021 and which asks *"the European Commission to strictly regulate the use of biometric technologies in order to avoid undue interference with fundamental rights"*. It appeals in particular to *"the Commission to prohibit, in law and in practice, indiscriminate or arbitrarily-targeted uses of biometrics which can lead to unlawful mass surveillance"*, clarifying that *"these intrusive systems must not be developed, deployed (even on a trial basis) or used by public or private entities insofar as they can lead to unnecessary or disproportionate interference with people's fundamental rights"*.[271]

Other initiatives from non-governmental organisations include complaints to data protections authorities[272], legal proceedings[273] and citizens' information. For example, Statewatch published a document which explains the concerns raised by biometric identity cards[274]. In France, several organisations have created the *"Technopolice"* platform[275], which aims to *"document, as rigorously as possible, the deployment of surveillance projects across the country, and build together tools and mobilisation strategies that make it possible to defeat them"*[276]. The association La Quadrature du Net clarifies that *"the issue is to succeed in organising local resistance, binding together initiatives so that they can feed into each other"* 277. A project of a similar nature was afterwards created in Belgium[278]. Several organisations also propose training to privacy protection and security, which however mostly focus on online threats[279].

Even though a part of the service industry endeavours to propose a positive image of biometric technologies[280] and may not hesitate to market free trials for public officers[281], other stakeholders defend the neutrality of some services. For example, several key representatives of the service industry such as Amazon, Google, Microsoft, Atlassian, Cisco, and IBM published *"Trusted Cloud Principles"*[282] by which they notably call governments to *"seek data directly from enterprise customers rather than cloud service providers, other than in exceptional circumstances"* and to ensure transparency toward customers, through specific notice, in case government access their data. These cloud providers also claim to be granted with a right to *"Protect Customers' Interests"*[283].

Nationally, individuals react to a lesser or a greater extent depending on their culture[284] and the political context. In some countries such as in France and Romania, the way national debates around the implementation of surveillance technology are conducted, as well as the insistence of public authorities in repeatedly proposing measures previously rejected by supreme courts, seem to trigger some degree of lassitude from citizens, who harbour feelings of disempowerment which, in turn, diminish their capability to complain.[285]

These circumstances do not prevent certain authorities[286] and public representatives[287] from claiming a democratic debate around the use of biometric technology. Civil contestations[288] and statutory declarations from representatives of political or public institutions are also observed. For example, No I Chahid-Nourai, former State Councillor and Member of the French Data Protection Authority, encouraged everyone to write and complain against the processing of a unique national number assigned to individuals, believing that there is no fatalism[289]. In 2012, when the French State was planning to implement a biometric identity card, a political representative stated: *"No democracy dared to take this step. Who can believe that legal guarantees […] are infallible?"*[290].

However, these statements are often silenced by the speed with which decisions are made before the European or national parliaments, when not altogether decided based on emergency ordinances – a situation particularly noticeable during the Covid-19 pandemic[291].

In this context, the fight for the preservation of freedoms essentially takes the form of initiatives from individuals and decentralised groups of citizens. This echoes a study by Goffman ([1961]) saying that *"when individuals feel that surveillance is wrong, or that they are unfairly disadvantaged by it, it will often be challenged"*[292].

These initiatives mostly focus on online privacy preservation, since offline control is more difficult to circumvent. A first group of projects aim to develop resistance tools and strategies, such as the TOR project[293] and other applications that enable end-to-end encrypted communication[294] or storage[295]. In relation to video-surveillance, Gary T. Marx reports eleven forms *"of resistance or non-compliance"*, including *"avoidance"* of places that are monitored and *"masking"*, to avoid being recognised[296]. In the same line, some artists, designers, and start-ups develop dresses, hairdressing, and make-up that aims to prevent facial recognition[297].

Other initiatives focus on the dissemination of information on threats and on practical ways to enhance one's data security and confidentiality. For example, the CryptoParty movement aims *"to pass on knowledge about protecting [oneself] in the digital space"*[298]. The Exodus project aims to *"analyse privacy concerns in Android applications"*[299]. It was developed in collaboration[300] with the *"Privacy Lab"* initiative of the Information Society Project at Yale Law School, which *"explores the connection between privacy, security, and anonymity through hands-on software and hardware implementation, such as cybersecurity workshops"*[301]. The noyb project aims to merge, into *"a stable European enforcement platform"*, *"best practices from consumer rights groups, privacy activists […] and legal tech initiatives"*[302]. Some other websites provide information on the use of encryption[303] or a list of available privacy enhancing tools[304].

102. The use of biometrics was evoked first in the decision of 8 June 2004 establishing the Visa Information System (VIS), see below footnote n°108. See also Ayse Ceyhan, 'Les technologies européennes de contrôle de l'immigration – Vers une gestion électronique des "personnes à risque"', Réseaux 2010/1 (n° 159), p. 131-150, published online on 1st February 2010, https://www.cairn.info/revue-reseaux-2010-1-page-131.htm.

103. Council regulation n° 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004R2252. See also the summary of this regulation at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14154.

104. Regulation (EU) 2019/1157 of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1157.

105. Regulation n°603/2013 of 26 June 2013 provides for the purpose of comparing with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purpose. In relation to purposes' extension, see below footnotes 108 to 110

106. Answer given by Mr Avramopoulos on behalf of the European Commission to a question for written answer from Cornelia Ernst (GUE/NGL): https://www.europarl.europa.eu/doceo/document/E-8-2018-001595-ASW_EN.html (see the Annex at https://www.europarl.europa.eu/RegData/questions/reponses_qe/2018/001595/P8_RE(2018)001595(ANN)_XL.pdf). Text of the question: https://www.europarl.europa.eu/doceo/document/E-8-2018-001595_EN.html.

107. European Agency for the Operational Management of Large-Scale IT Systems in the area of freedom, security and justice, https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems.

108. The Visa Information System (VIS), established by a Council decision of 8 June 2004, is a common identification system for visa data, which enables "authorised national authorities to enter and update visa data and to consult these data electronically" (see the Decision of the Council, reason n°1 and art. 1§1, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32004D0512). Conditions and procedures for the exchange of data were established by Regulation (EC) n° 767/2008 of the European Parliament and of the Council of 9 July 2008 (VIS Regulation), which added, amongst the VIS purposes, the contribution "to the prevention of threats to the internal security of any of the Member States" (art. 2) as well as the "prevention, detection and investigation of terrorist offences and other serious criminal offences" (art. 3): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02008R0767-20190611.

109. The Schengen Information System (SIS) was initially set up pursuant to the Convention of 19 June 1990 implementing the Schengen Agreement. The development of the second generation of SIS (SIS II) is based on Council Regulation (EC) n° 2424/2001, Council Decision 2001/886/JHA, Regulation (EC) n° 1987/2006 and Council Decision 2007/533/JHA. Initially established for the purpose of gradually suppressing checks at common borders, the purposes of ensuring "a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security […] and the safeguarding of security in the territories of the Member States" was added by Regulation (EC) n° 1987/2006. The latter was repealed together with the Council Decision of 2007, by Regulation (EU) 2018/1862 of 28 November 2018, which extends the use of SIS II to "the field of police cooperation and judicial cooperation in criminal matters": https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1862.

110. Eurodac is a fingerprint database established for the comparison of fingerprints for the effective application of the Dublin Convention, which determines the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities (see Council Regulation (EC) n°2725/2000 of 11 December 2000 concerning the establishment of Eurodac, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32000R2725 and the Council Regulation n° 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002R0407). Regulation n°603/2013 of 26 June 2013 adds the 2nd purpose of comparing with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0603. The intent to enable this second Eurodac purposes was first revealed in 2008, see the Opinion of the European Data Protection Supervisor (EDPS) n° 2011/C 101/03 of 15 December 2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:101:0014:0019:EN:PDF.

111. The European Criminal Records Information System (ECRIS), operational since April 2012, which "provides an electronic exchange of criminal record information on a decentralised basis between Member States", https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn, was improved with the adoption of Regulation (EC) n° 2019/816 of 17 April 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0816.

112. The ETIAS system is a pre-travel authorisation system for visa exempt travellers, https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Etias.

113. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history. The Entry/Exit System (EES) was developed to further improve the management of the external borders: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/EES

114. These softwares are SafranAFIS, Accenture Middleware and WorkFlow Integration, Oracle Database Morpho Biometric Search Services (MBSS)

by IDEMIA; RabbitMQ and Linux. Softwares used by the Europol database are Windows Server 2012 and a custom Automated Biometric Identification System (ABIS) by SopraSteria. See Answer given by Mr Avramopoulos on behalf of the European Commission to a question for written answer from Cornelia Ernst (GUE/NGL), already mentioned.

115. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history.

116. Answer given by Mr Avramopoulos on behalf of the European Commission to a question for written answer from Cornelia Ernst (GUE/NGL), already mentioned.

117. Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa), COM/2017/0793 final - 2017/0351 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0793.

118. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0817 and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.135.01.0085.01.ENG. Regulation (EU) 2021/1133 of 7 July 2021 lays down the manner in which interoperability and the conditions for the consultation of the data stored are to be implemented: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R1133.

119. Erick Haehnsen, Classement des pays selon leur utilisation des données biométriques, 4 December 2019, https://www.infoprotection.fr/classement-des-pays-selon-leur-utilisation-des-donnees-biometriques/.

120. Articles 2 of Regulations (EC) n° 2019/817 and n° 2019/818 organise interoperability for "these EU information systems and their data to supplement each other", in a series of purposes including prevention and combating illegal immigration and contributing to a high level of security within the area of freedom, security and justice of the Union, including "the maintenance of public security […], the prevention, detection and investigation of terrorist offences and other serious criminal offences" and "the identification of unknown persons […] in the case of a natural disaster, accident or terrorist attack".

121. Frank Hersey, 'EU members launch new biometric ID applications on deadline day', 5 August 2021, https://www.biometricupdate.com/202108/eu-members-launch-new-biometric-id-applications-on-deadline-day.

122. Regulation (EU) 2019/1157 of 20 June 2019, already mentioned, art. 10.

123. Article 10 and recitals 21 and 22 of Regulation 2019/1157. See also subsections 4.2 and 4.3 of the current study.

124. In relation to Poland, see Luca Montag et al., The rise and rise of biometric mass surveillance in the EU, EDRi, 2021, https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf. See in particular p. 14 and p.120. France partly based the creation of its central database by reference to the SIS II legislation, see subsection 7.1.2 of the current study.

125. For example France, Belgium, Denmark, The Netherlands and Sweden: Sénat, Le numéro unique d'identification des personnes physiques', Étude de législation comparée, n° 181, December 2007, https://www.senat.fr/lc/lc181/lc181_mono.html.

126. For example Spain, Italy and Switzerland: Sénat, 'Le numéro unique d'identification des personnes physiques', already mentioned.

127. Such as in Romania, see subsection 7.3.1.1 of the current study.

128. In addition to previous paragraphs under the current subsection, see for example the cases of France, Romania and the United Kingdom, in subsections 7.1.1.2, 7.2.1.2 and 7.3.1.2 of the current study.

129. A study released in 2021 argues that "54% of the world's 770 million surveillance cameras are situated in China, meaning there are approximately 415.8 million located in the country": Paul Bischoff, 'Surveillance camera statistics: which cities have the most CCTV cameras?', 17 May 2021, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/. This author estimate that "China's CCTV camera count could rise to as much as 540 million" one year from the study. These estimates seem in line with a study from 2019 which recorded 200 millions of camera in 2019: Humza Aamir, 'Report finds the US has the largest number of surveillance cameras per person in the world', 6 December 2019, https://www.techspot.com/news/83061-report-finds-us-has-largest-number-surveillance-cameras.html.

130. Benjamin J. Goold, 'CCTV and Human Rights', in European Forum for Urban Security, Citizens, Cities and Video Surveillance: Towards a democratic and responsible use of CCTV, June 2010, p. 27, https://panoptykon.org/sites/panoptykon.org/files/cctv_publication_en_0.pdf. For town-specific studies, see for example Pauline De Keersmaecker et Corentin Debailleul, The spatial distribution of open-street CCTV in the Brussels-Capital Region, Brussels Studies, 2016, https://journals.openedition.org/brussels/1427;

131. CCTV systems may be run by local or municipal police forces or be the result of a public-private partnership. The allocated budget may come from the local community's resources or be partly covered by the state, based on an allocated budget, associated or not with guidelines in terms of use: Eric Töpfer, 'Urban Video Surveillance in Europe: A Political Choice?', in European Forum for Urban Security, Citizens, Cities and Video Surveillance: Towards a democratic and responsible use of CCTV, June 2010, p. 65-79, see especially p.73-78, https://panoptykon.org/sites/panoptykon.org/files/cctv_publication_en_0.pdf. See also our analysis of the French context, in subsection 7.1.1.1 of the current study.

132. Paul Bischoff, 'Surveillance camera statistics: which cities have the most CCTV cameras?', 17 May 2021, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ . See also Ma Forteresse, 'Vidéosurveillance : Histoire de la caméra de surveillance', https://www.maforteresse.com/guide/videosurveillance-histoire-de-la-camera-de-surveillance.html#Quelques_chiffres_sur_lutilisation_actuelle_de_la_camera_de_surveillance, which

evokes a ratio of 68,4 cameras for 1,000 inhabitants.

133. Paul Bischoff, 'Surveillance camera statistics: which cities have the most CCTV cameras?', already mentioned.

134. Ma Forteresse, 'Vidéosurveillance : Histoire de la caméra de surveillance', already mentioned.

135. "The surveillance industry is worth 36,89 billion of dollars and will rise up to 68,39 billion of dollars within 5 years (according to Les Echos magazine)" (translated from French): Ma Forteresse, 'Vidéosurveillance : Histoire de la caméra de surveillance', already mentioned.

136. See subsection 3.2 of the current study.

137. "GoogLeNet is a type of convolutional neural network based on the Inception architecture. It utilises Inception modules, which allow the network to choose between multiple convolutional filter sizes in each block. An Inception network stacks these modules on top of each other, with occasional max-pooling layers with stride 2 to halve the resolution of the grid": definition introduced by Szegedy et al. in Going Deeper with Convolutions, https://paperswithcode.com/method/googlenet. Link to the original publication: https://paperswithcode.com/paper/going-deeper-with-convolutions.

138. Dominique Verdejo and Eunika Mercer Laurent, 'Video intelligence as a component of a global security system', in Artificial Intelligence for Knowledge Management, 2017, hal-02384839, n° 3.1, https://hal.archives-ouvertes.fr/hal-02384839.

139. Luca Montal et al., The Rise and Rise of Biometric Mass Surveillance in the EU: A Legal Analysis of Biometric Mass Surveillance Practices in Germany, The Netherlands and Poland, EDRI, 7 July 2021, respectively p. 19 and p. 60, https://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf. See also Ella Jakubowska, 'New EDRi report reveals depths of biometric mass surveillance in Germany, the Netherlands and Poland', 7 July 2021, https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/.

140. See subsection 7.2.1.1 of the current study.

141. See subsection 7.1.1.1 of the current study.

142. See subsection 7.3.1.1 of the current study.

143. As shown, for example, by Paul Bischoff, 'Biometric data: 96 countries ranked by how they're collecting it and what they're doing with it', 27 January 2021, https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/ and other country-specific studies such as Laura Carrer et al., 'How facial recognition is spreading in Italy: the case of Como', 17 September 2020, https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como. The EU policy in relation to the implementation of biometrics in travel documents further implies the use of biometrics for border control at least.

144. See in this regard the supporting policy of the European Union to the development of this technology in Western Balkans, in subsection 3.2 of the current study. It is also reported that Serbia "has deployed enough biometric surveillance technology from China's Huawei for law enforcement and "Safe City" solutions to cover practically all of Belgrade's public spaces": Danilo Krivokapić, Mila Bajić and Bojan Perkov, 'Biometrics in Belgrade: Serbia's path shows broader dangers of surveillance state', 19 May 2021, http://www.eu.boell.org/en/2021/05/19/biometrics-belgrade-serbias-path-shows-broader-dangers-surveillance-state. See also Manuel G. Pascual, 'El reconocimiento facial chino llega a las puertas de la Unión Europea', 18 June 2021, https://elpais.com/tecnologia/2021-06-18/el-reconocimiento-facial-chino-llega-a-las-puertas-de-la-union-europea.html?event_log=fa&prod=REG&o=CABEP; Pierre Demoux, 'Le « Big Brother » chinois arrive aux portes de l'Europe', 21 June 2021, https://www.lesechos.fr/idees-debats/editos-analyses/le-big-brother-chinois-arrive-aux-portes-de-leurope-1325323.

145. See subsection 7.1.1.1, 7.2.1.1 and 7.3.1.1 of the current study.

146. In Italy, body-worn cameras have already been experimented for several years by LEA: see Polizia di Statto, 'Microcamere agli agenti delle Volanti e della Stradale', 15 June 2015, https://www.poliziadistato.it/articolo/microcamere-agli-agenti-delle-volanti-e-della-stradale.

147. On the use of body-worn cameras in Greece, see Amnesty International, Greece, Freedom of Assembly at risk and unlawful use of force in the era of Covid-19, 2021, p. 14, https://policehumanrightsresources.org/content/uploads/2021/07/GREECE_FREEDOM-OF-ASSEMBLY-AT-RISK-AND-UNLAWFUL-USE-OF-FORCE-IN-THE-ERA-OF-COVID-19.pdf?x96812.

148. See subsection 7.3.1.1 of the current study.

149. 'Paramedic Safety Prioritized: London Ambulance Service Rolls Out Body-Worn Camera Solution From Motorola Solutions', 23 February 2021, https://newsroom.motorolasolutions.com/news/paramedic-safety-prioritized-london-ambulance-service-rolls-out-body-worn-camera-solution-from-motorola-solutions.htm.

150. This model is used by law enforcement agencies in France, England and Romania, see subsections 7.1.1.1 and 7.2.1.1 and 7.3.1.1 of the current study.

151. See subsection 7.1.1.1, 7.2.1.1 and 7.3.1.1 of the current study.

152. 'Italy: Garante approves use of body worn cameras by law enforcement but bans facial recognition', 28 September 2021, https://www.dataguidance.com/news/italy-garante-approves-use-body-worn-cameras-law; 'Garante per la Protezione dei Dati Personali (GPDP), Body cam: ok dal Garante privacy, ma no al riconoscimento facciale', Newsletter n°. 481 of 10 September 2021, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9698442#1.

153. See subsections 7.1.1.1, 7.2.1.1 and 7.3.1.1 of the current study.

154. Chen Lin (Reporting) and Marguerita Choy (edition), 'Singapore trials patrol robots to deter bad social behaviour, 6 September 2021', Reuters, https://www.reuters.com/technology/singapore-trials-patrol-robots-deter-bad-social-behaviour-2021-09-06/.

155. OECD, International Transport Forum, Covid-19 Transport Brief: Drones in the Era of Coronavirus, 19 June 2020, p. 3, https://www.itf-oecd.org/sites/default/files/drones-covid-19.pdf; see subsection 7.1.1.1 and 7.2.1.1 of the current study.

156. CNIL, 'Drones : la CNIL sanctionne le ministère de l'Intérieur', 14 January 2021, https://www.cnil.fr/fr/

drones-la-cnil-sanctionne-le-ministere-de-linterieur. See also subsections 7.1.1.1 and 7.1.2 of the current study; Rick Noack, 'In victory for privacy activists, France is banned from using drones to enforce coronavirus rules', 14 January 2021,The Washington Post, https://www.washingtonpost.com/world/in-victory-for-privacy-activists-france-is-banned-from-using-drones-to-enforce-covid-rules/2021/01/14/b384eb40-5658-11eb-acc5-92d2819a1ccb_story.html.

157. See subsection 3.2 of the current study.

158. See subsection 7.3.1.1 of the current study.

159. Ryan Mac, Caroline Haskins and Antonio Pequeño IV, 'Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here', 25 August 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

160. Philippe Reltien, 'Reconnaissance faciale : officiellement interdite, elle se met peu à peu en place', 5 September 2020 (update), France Inter, https://www.franceinter.fr/reconnaissance-faciale-officiellement-interdite-elle-se-met-peu-a-peu-en-place.

161. Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 59; See also subsection 7.1.1.1 of the current study.

162. Philippe Reltien, 'Reconnaissance faciale : officiellement interdite, elle se met peu à peu en place', already mentioned.

163. In 2021, main providers of CCTV technology were identified, all regions of the world considered, to be the following: Hangzhou Hikvision Digital Technology Co Ltd, Zhejiang Dahau Technology Co. Ltd, Honeywell International Inc, Axis Communications AB, Pelco Inc, Bosch Security Systems, Inc, Panosonic System Network Co. Limited, Toshiba Corporation, Hanwha Techwin Co. Ltd and Geovision Inc: MarketWatch, "Closed Circuit Television (CCTV) Camera Market Size In 2021 with Top Countries Data: What is the trajectory for the Closed Circuit Television (CCTV) Camera Industry growth (CAGR) in the forecast period (2021-2026)?", Press release, 27 August 2021, https://www.marketwatch.com/press-release/closed-circuit-television-cctv-camera-market-size-in-2021-with-top-countries-data-what-is-the-trajectory-for-the-closed-circuit-television-cctv-camera-industry-growth-cagr-in-the-forecast-period-2021-2026-latest-98-pages-report-2021-08-27. Another study, relating to Germany, mentions the following biometric softwares providers: Dallmeier, Cognitec, Clairview AI, Videmo, Idemia: Luca Montal et al., The Rise and Rise of Biometric Mass Surveillance in the EU: A Legal Analysis of Biometric Mass Surveillance Practices in Germany, The Netherlands and Poland, EDRI, 7 July 2021, p. 23-30, https://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf.

164. IDEMIA results in the merger of OT (Oberthur Technologies) et Safran Identity & Security (Morpho). With revenues of nearly 3 billion euros, it counts 14,000 employees in more than 180 countries. See IDEMIA, 'OT-Morpho becomes IDEMIA, the global leader in trusted identities', 28 September 2017, https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28.

165. Nacer Lalam and Franck Nadaud, 'La biométrie : un secteur rentable soutenu par la commande publique', in Ayse Ceyhan and Pierre Piazza, L'identification biométrique : Champs, acteurs, enjeux et controverses, Éditions de la Maison des Sciences de l'Homme, 2011, p. 81-99, p. 81.

166. For example, in Romania, Echogroup provided a surveillance solution to the city of Slatina (Elko, 'Video surveillance system for Slatina city in Romania', https://www.elkogroup.com/cases/video-surveillance-system-for-slatina-city-in-romania). In Paris, the company Datakalab was chosen in order to implement, in the underground, a system to estimate the percentage of users wearing protective face mask (Xavier Demagny, 'Paris : des «caméras intelligentes» pour estimer le nombre de voyageurs sans masque', 9 May 2020 (update), France Inter, https://www.franceinter.fr/societe/paris-des-cameras-intelligentes-pour-estimer-le-nombre-de-voyageurs-sans-masque).

167. Nacer Lalam and Franck Nadaud, 'La biométrie : un secteur rentable soutenu par la commande publique', already mentioned, p. 81.

168. See subsection 4.2 of the current study.

169. In 2013, Google discovered that the French National Authority for Information Systems Security (ANSSI) issued fraudulent certificates, which enabled the authority to intercept communications addressed to Google servers: Valéry Marchive, 'Google découvre de faux certificats émis par l'Anssi', 10 December 2013, https://www.lemagit.fr/actualites/2240210797/Google-decouvre-de-faux-certificats-emis-par-lAnssi. In 2013, Edward Snowden revealed that the intelligence services of several coutries collected citizens' communications metadata outside any legal framework, see subsections 7.2.1.2.1 and 7.3.1.3 of the current study.

170. Alessandro Mascellino, 'Global facial recognition market expected to grow 12 percent to 2025 – report, 7 September 2021', https://www.biometricupdate.com/202109/global-facial-recognition-market-expected-to-grow-12-percent-to-2025-report. In relation to the CCTV industry, a study mentions that "the surveillance industry is worth 36,89 billion of dollars and will rise up to 68,39 billion of dollars within 5 years (according to Les Echos magazine)": Ma Forteresse, 'Vidéosurveillance : Histoire de la caméra de surveillance', https://www.maforteresse.com/guide/videosurveillance-histoire-de-la-camera-de-surveillance.html#Quelques_chiffres_sur_lutilisation_actuelle_de_la_camera_de_surveillance.

171. See subsection 7.1.1.2. of the current study.

172. For example, the Romanian National Institute for Research and Development in Informatics (ICI) Bucharest is involved in a public service digital identity project in partnership with a Romania-based firm in order to digitalise the national public system and enable "individuals' interaction with government institutions" through a "decentralised digital identity platform": Alessandro Mascellino, 'Public service digital identity projects unveiled by Gradiant, ICI Bucharest and selfd.id', 19 February 2021, https://www.biometricupdate.com/202102/public-service-digital-identity-projects-unveiled-by-gradiant-ici-bucharest-and-selfd-id. See subsection 7.3.1.3 of the current study.

173. Tifaine Mariotte, 'La biométrie : un outil en constante évolution dans les entreprises', 7 April 2021, https://portail-ie.fr/analysis/2806/la-biometrie-un-outil-en-constante-evolution-dans-les-entreprises.

174. The French banks BNB Paribas and Crédit Agricole,

use a technology based on fingerprints to improve "transactions fluidity and security" (BNP using a THALES technology): Pascal Perriot, 'Le paiement par carte bancaire biométrique, sans contact et au-delà de 50 € : c'est pour la rentrée 2021 !', 3 September 2021, https://www.snacking.fr/actualites/management-franchise/5711-Le-paiement-par-carte-bancaire-biometrique-sans-contact-et-au-dela-de-50-c-est-pour-la-rentree-2021-/; Ayang Macdonald, 'FPC plans for biometric payment, access and mobile growth; opens regional offices', 12 April 2021, https://www.biometricupdate.com/202104/fpc-plans-for-biometric-payment-access-and-mobile-growth-opens-regional-offices. The Bulgarian Raiffeisenbank, uses face recognition technology https://paybyface.io, which would enable the bank "to evaluate the attitudes of Bulgarian consumers towards payments authorized and secured by facial recognition": Chris Burt, PayByFace, 'VisionLabs face biometrics deployments for retail payments showcase regional demand', 10 May 2021, https://www.biometricupdate.com/202103/paybyface-visionlabs-face-biometrics-deployments-for-retail-payments-showcase-regional-demand.

175. Alessandro Mascellino, 'Biometrics to replace car keys for Genesis vehicle, Cerence voice control deployed by VinFast', 30 September 2021, https://www.biometricupdate.com/202109/biometrics-to-replace-car-keys-for-genesis-vehicle-cerence-voice-control-deployed-by-vinfast.

176. See for example the Windows Hello feature: https://support.microsoft.com/fr-fr/windows/d%C3%A9couvrir-puis-configurer-windows-hello-dae28983-8242-bb2a-d3d1-87c9d265a5f0.

177. Department for education, Protection of biometric information of children in schools and colleges, March 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf.

178. Sarah Boumghar, 'Des collèges et lycées utilisent-ils des dispositifs biométriques pour contrôler l'accès à la cantine ?', 17 September 2019, https://www.liberation.fr/checknews/2019/09/17/des-colleges-et-lycees-utilisent-ils-des-dispositifs-biometriques-pour-controler-l-acces-a-la-cantin_1748971/;

179. See examples in France and in Romania, in subsections 7.1.1.2 and 7.3.1.2 of the current study.

180. Erick Haehnsen, 'La biométrie comportementale en voie vers la maturité', 29 April 2021, https://www.infoprotection.fr/la-biometrie-comportementale-en-voie-vers-la-maturite/; Ségolène Kahn, 'L'authentification en continu, une réponse aux failles de la biométrie ?', 29 October 2020, https://www.infoprotection.fr/lauthentification-en-continu-une-reponse-aux-failles-de-la-biometrie/.

181. See for example the CyAN Guidance on Use of Invigilation Software by Educational Institutions, 6 June 2020, https://cyan.network/blog/2020/06/06/cyan-guidance-on-use-of-invigilation-software-by-educational-institutions/.

182. For example, a Smart Interactive Advertising Board (SIAB) was designed in 2013, offering the possibility to determine displays according to "user position, location, and movements": Baker Alrubaiey et al., 'Smart interactive advertising board (SIAB)', August 2013, Conference paper, Advanced Applied Informatics (IIAIAAI), 2013 IIAI International Conference on Advanced Applied Informatics, https://ieeexplore.ieee.org/document/6630366. The company Yahoo! is also reported to have registered "a patent describing a 'smart' advertising board: equipped with sensors, microphones, cameras and retinal scanners": Numendil, 'Yahoo réfléchit à des panneaux d'affichage intelligents qui vous regardent et vous écoutent', 3 November 2016, https://pixellibre.net/2016/11/yahoo-reflechit-panneaux-daffichage-intelligents-regardent-ecoutent/.

183. Such as Google or Yahoo. In addition, it appears that the Snowden revelations showed that "Britain's surveillance agency GCHQ, with aid from the US National Security Agency, intercepted and stored the webcam images of millions of internet users not suspected of wrongdoing", between 2008 and 2010, using "a surveillance program codenamed Optic Nerve [which] collected still images of Yahoo webcam chats in bulk and saved them to agency databases": Spencer Ackerman and James Ball, 'Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ', 28 February 2014, The Guardian, https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

184. See for example the case of Microsoft's Cortana (https://support.microsoft.com/en-us/topic/what-can-you-do-with-cortana-in-windows-f57ef46f-716a-9940-a8fc-09b3433d05ea) and of Amazon's Alexa (https://press.aboutamazon.com/alexa-features).

185. P.B. avec AFP, 'Astro, le petit robot controversé d'Amazon capable de patrouiller dans la maison', 29 September 2021, https://www.20minutes.fr/high-tech/3135711-20210929-astro-petit-robot-controverse-amazon-capable-patrouiller-maison.

186. European Commission, 'Smart Metering deployment in the European Union', 1st October 2021, https://ses.jrc.ec.europa.eu/smart-metering-deployment-european-union.

187. Ariana DiValentino, 'Proof of COVID-19 vaccination is required at some music venues, sports arenas, and airlines — these are the best vaccine passport apps to download', 2 August 2021, https://www.insider.com/best-vaccine-passport-apps.

188. IMeasureU, 'Sport Movement Analysis - Sports Science On The Rise', https://imeasureu.com/knowledge/sport-movement-analysis/.

189. RomanTrobec et al., System for Mobile Monitoring of Vital Functions and Environmental Context, Procedia Technology, Volume 27, 2017, Pages 157-158, https://www.sciencedirect.com/science/article/pii/S2212017317300695.

190. Alexandre Chen, 'Gérer les données personnelles fournies aux applications', in I2D - Information, données & documents 2017/3 (Volume 54), p. 47-48, https://www.cairn.info/revue-i2d-information-donnees-et-documents-2017-3-page-47.htm.

191. Jacob Leon Kröger, Philip Raschke, Towhidur Rahman Bhuiyan, Privacy Implications of Accelerometer Data: A Review of Possible Inferences, 2019, ACM, https://dl.acm.org/doi/pdf/10.1145/3309074.3309076.

192. Jacob Leon Kröger, Philip Raschke, Towhidur Rahman Bhuiyan, Privacy Implications of Accelerometer Data: A Review of Possible Inferences, already mentioned.

193. Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 13, referring to a study performed in 2017 by Dscout.

194. We can refer to the providers Cozy Cloud (https://cozy.io/en/), Greenbureau (https://particulier.greenbureau.fr/), Paid That (https://ipaidthat.io/fr/) and Digiposte (https://www.laposte.fr/digiposte/tous-mes-documents-partout-et-tout-le-temps). Indeed, these providers do not appear to propose "end-to-end encryption", which is however the only means to ensure that they cannot themselves access the stored information.

195. See for example https://support.cozy.io/article/120-combien-de-connecteurs-sont-aujourd-hui-disponibles-dans-cozy; https://www.numendo.com/blog/data/solid-un-cloud-prive-qui-vous-redonne-le-pouvoir-sur-vos-donnees/.

196. End-to-End encryption refers to "systems which encrypt a message in-transit so that only the devices at either end of the exchange have access to the keys required to decrypt the data": Ksenia Ermoshina and Francesca Musiani, 'Hiding from whom?: Threat-models and in-the-making encryption technologies', in History and Theory of the Arts, Literature and Technologies, Erudit, 2018, Cacher/Concealing, DOI: 10.7202/1058473ar, halshs-02320706, https://hal.archives-ouvertes.fr/halshs-02320706. As a result, end-to-end encryption prevents anyone else but the sender or the recipient from reading the content of the message.

197. See subsection 4.2.2 of the current study.

198. See subsection 4.2 of the current study.

199. Shoshana Zuboff, The age of surveillance capitalism, The fight for a human future at the new frontier of power, ed. Profile Book, 2019.

200. Olivier Koch, 'Les données de la guerre. Big Data et algorithmes à usage militaire', in Les Enjeux de l'information et de la communication, 2018/2 (N° 19/2), p. 113-123, https://www.cairn.info/revue-les-enjeux-de-l-information-et-de-la-communication-2018-2-page-113.htm.

201. Translated from French: Sylvia Preuss-Laussinotte, 'L'Union européenne et les technologies de sécurité', in Cultures et Conflits, n°64 Identifier et Surveiller – Hiver 2006, p. 97-108, n° 1, https://doi.org/10.4000/conflits.2123.

202. Translated from French: Sylvia Preuss-Laussinotte, 'L'Union européenne et les technologies de sécurité', already mentioned.

203. Sylvia Preuss-Laussinotte, 'L'Union européenne et les technologies de sécurité', already mentioned, n° 6. See also, for example, 'Société de la connaissance, société de l'information, société de contrôle. Entretien avec Armand Mattelart', in Cultures & Conflits, n°64 Hiver 2006 (4/2006), pp. 167-183, n°22, https://journals.openedition.org/conflits/2051.

204. European Commission, 'European Commission launches Digital Agenda for the Western Balkans', 25 June 2018, Press release, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4242.

205. Translated from French: Sophie-Anne Bisiaux and Lorenz Naegeli, 'Chantage dans les Balkans : comment l'UE externalise ses politiques d'asile', 7 July 2021, https://www.ritimo.org/Chantage-dans-les-Balkans-comment-l-UE-externalise-ses-politiques-d-asile.

206. Question for written answer E-002257/2021 from Özlem Demirel (The Left) to the Commission, 27 April 2021, https://www.europarl.europa.eu/doceo/document/E-9-2021-002257_EN.html. See also Statewatch, 'Council Presidency and EU agencies want biometric databases for migrants and refugees in the Western Balkans', 26 February 2020, https://www.statewatch.org/news/2020/february/council-presidency-and-eu-agencies-want-biometric-databases-for-migrants-and-refugees-in-the-western-balkans/.

207. Sylvia Preuss-Laussinotte, 'L'Union européenne et les technologies de sécurité', in Cultures et Conflits, n°64 Identifier et Surveiller – Hiver 2006, p. 97-108, n° 8, https://doi.org/10.4000/conflits.2123. See also EDRI, 'Biometrics in EU passports', 2 July 2003, https://edri.org/our-work/edrigramnumber12biometrics/: "In a remarkably high-speed procedure, the EU Council plans to oblige all Member States of the Union to introduce chips containing biometric data on their passports within little less than a year. Allegedly, this step is taken to meet a U.S. deadline set on 26 October 2004. After that date, according to a law passed eight months after the 11 September attacks, the U.S will demand visas from all travellers entering the U.S. who don't have DNA code, fingerprints, or iris scans embedded in their travel documents".

208. On this issue see also Daniel J. Solove, Nothing to Hide: The false Tradeoff between Privacy and Security, Yale, University Press, New Haven and London, May 2011, Introduction p. 2, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1827982.

209. Translated from French: Sylvia Preuss-Laussinotte, 'L'Union européenne et les technologies de sécurité', already mentioned., n°8. The author explains, in n °9-11, that the recourse to biometry against terrorism is evoked in 2002 in a NATO report, and that the ICAO, in direct link with the ISO, have played a central role in the design and definition of biometric norms that are applicable in Europe. These norms have been imposed on states bound to the Chicago Convention for reasons of air transport safety.

210. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 133.

211. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.133.

212. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.133.

213. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.135.

214. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.134-135.

215. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.133.

216. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.151.

217. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.151. In relation to historical examples, see the introduction of the current report.

218. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.141. The authors explain especially that, at the EU and the UK level, "not a single feasibility study or technology study was introduced to inform parliamentarians about the advantages, disadvantages, or potential failure […]. The common view […] was that because the technology was approved by UN bodies […]. The ICAO did not scrutinize the technology in details either, however. [One of its members] admitted that […] they were unsure of the abilities of the technology to match their goal" (Edgar A. Whitley and Gus Hosein, already mentioned, p. 140).

219. Translated from French: Sylvia Preuss-Laussinotte, 'L'Union européenne et les technologies de sécurité', already mentioned, n°13. SAGEM is an enterprise involved in the development of biometrics and identity documents.

220. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.125, referring to Gus Hosein's previous works.

221. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p. 125s.

222. A large part of EU Member States implemented the biometric ID card the day of the EU deadline: Frank Hersey, 'EU members launch new biometric ID applications on deadline day', 5 August 2021, https://www.biometricupdate.com/202108/eu-members-launch-new-biometric-id-applications-on-deadline-day.

223. See for example, in relation to France, subsection 7.1.1.3 of the current study.

224. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p.127: "Throughout the Parliamentary debate the government frequently referred to the "international obligations" on the UK to update its travel documents":

225. Jorge Valero and Samuel Stolton, 'EU leaders to call for an EU electronic ID by mid-2021', 9 September 2020, https://www.euractiv.com/section/digital/news/eu-leaders-to-call-for-an-eu-electronic-id-by-mid-2021/.

226. See subsection 5.1.4.1 of the current study.

227. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 35 s., https://hal.archives-ouvertes.fr/tel-02439529.

228. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, already mentioned, p. 37.

229. Guillaume Gormand, already mentioned, p. 39.

230. Guillaume Gormand, already mentioned, p. 37.

231. Translated from French: Guillaume Gormand, already mentioned, p. 41.

232. Translated from French: Guillaume Gormand, already mentioned, p. 41.

233. Translated from French: Guillaume Gormand, already mentioned, p. 45.

234. Translated from French: Guillaume Gormand, already mentioned, p. 44.

235. Translated from French: Guillaume Gormand, already mentioned, p. 48.

236. Translated from French: Guillaume Gormand, already mentioned, p. 45 ; Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', Note du CREOGN, September 2019, p. 4, https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-creogn/reconnaissance-faciale-et-controles-preventifs-sur-la-voie-publique-l-enjeu-de-l-acceptabilite; Eric Töpfer, 'Urban Video Surveillance in Europe: A Political Choice?', in European Forum for Urban Security, Citizens, Cities and Video Surveillance - Towards a democratic and responsible use of CCTV, June 2010, p. 65-79, p. 78, https://panoptykon.org/sites/panoptykon.org/files/cctv_publication_en_0.pdf.

237. Ministère de l'Intérieur, 'La nouvelle carte nationale d'identité', 3 May 2021, https://www.interieur.gouv.fr/actualites/actu-du-ministere/nouvelle-carte-nationale-didentite: on this webpage, the French Ministry of Home Affairs states: "the new identity card will be more secure [and] more practical". Members of the French Senate have for their part evoked the existence of the industry data processing activities in order to justify the state's data processing activities: see subsection 7.1.1.3 of the current study.

238. Sylvia Preuss-Laussinotte, 'L'Union européenne et les technologies de sécurité', in Cultures et Conflits, n°64 Identifier et Surveiller – Hiver 2006, p. 97-108, n° 4, https://doi.org/10.4000/conflits.2123. See also Regulation (EU) 2019/1157 of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, reasons 5-10, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1157. See also the European Commission press release that promotes biometry through announcing that "New, secure biometric passports in the EU, strengthen security and data protection and facilitates travelling": Press release, 29 June 2006, https://ec.europa.eu/commission/presscorner/detail/en/IP_06_872.

239. "The argument [that biometry is irremediable] reduces the debate to a discussion on the technology deployment modalities" (translated from French): Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 58, referring to a note from a Colonel of the French Gendarmerie written in a review of the Centre of Research of the French National Gendarmerie Officers School (CREOGN): Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', already mentioned, n°43. The author further recognises that "recourse to facial recognition by law enforcement has the merit of being an enlightened choice of society" (translated from French).

240. See for example Regulation (EU) 2018/1862 of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1862, whose reason 1 evokes the Schengen Information System as "one of the major compensatory measures contributing to maintaining a high level of security within the area of freedom, security and justice of the Union».

241. *Most politicians present security as more important than freedom, or as the first of freedoms. For the example of France, subsection 7.1.3 of the current study.*

242. *Such a statement, which appears in all Directives and Regulations in the field, creates an impression of style statement, in the light of the low level of guarantees that are included in the above mentioned legal instruments. Some ECHR and EUCFR violations were further confirmed by the CJEU and the ECtHR. See for example, in relation to the data retention directive, CJEU, 'The Court of Justice declares the Data Retention Directive to be invalid', 8 April 2014, https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf, and EDRi, 'ECtHR: UK Police data retention scheme violated the right to privacy', 26 February 2020, https://edri.org/our-work/ecthr-uk-police-data-retention-scheme-violated-the-right-to-privacy/. On these issues see sections 4 and 5 of the current study.*

243. *See subsection 4.1 of the current study.*

244. *See subsection 5.2 of the current study.*

245. *See subsection 5.1.3 of the current study.*

246. *See subsection 4.1 of the current study.*

247. *See also subsection 7.1.1.3 of the current study.*

248. *See for example Mike Ball, 'EMSA Surveillance UAV Deployed in Romania', 17 November 2020, https://www.unmannedsystemstechnology.com/2020/11/emsa-surveillance-uav-deployed-in-romania/. See also Nathan Gain, 'Romanian Border Police operating CAMCOPTER S-100 RPAS for maritime surveillance', 8 April 2021, https://www.navalnews.com/naval-news/2021/04/romanian-border-police-operating-camcopter-s-100-rpas-for-maritime-surveillance/.*

249. *About Intel, Surveillance R&D, Discussion Prompt: Are civil liberties and democratic accountability sufficiently incorporated into the priorities of surveillance research programs?, https://aboutintel.eu/surveillance-rd/. Within the framework of this discussion, see especially Estelle De Marco, 'Ethics in surveillance research: from theory to practice', 21 October 2021, https://aboutintel.eu/ethics-in-surveillance-research-theory-to-practice/.*

250. *Cordis, European Commission, Seamless panoramic video surveillance in any environment, https://cordis.europa.eu/article/id/36383-seamless-panoramic-video-surveillance-in-any-environment.*

251. *Cordis, European Commission, Seamless panoramic video surveillance in any environment, already mentioned.*

252. *Cordis, Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment, https://cordis.europa.eu/project/id/218086. See also Fabien Soyez, 'INDECT : le projet de surveillance intelligente européen', 18 April 2013, https://www.cnetfrance.fr/news/indect-le-projet-de-surveillance-intelligente-europeen-39789260.htm.*

253. *Patrick Breyer, 'EU-funded technology violates fundamental rights', 22 April 2021, https://aboutintel.eu/transparency-lawsuit-iborderctrl/. See also the website https://www.iborderctrl.eu/.*

254. *Cordis, Intelligent Portable Border Control System, https://cordis.europa.eu/project/id/700626.*

255. *https://www.iborderctrl.eu/The-project.*

256. *Erick Haehnsen, 'Classement des pays selon leur utilisation des données biométriques', 4 December 2019, https://www.infoprotection.fr/classement-des-pays-selon-leur-utilisation-des-donnees-biometriques.*

257. *Cordis, Identity Management in PUbLic Services, https://cordis.europa.eu/project/id/101004459.*

258. *Amnesty International, 'EU companies selling surveillance tools to China's human rights abusers', 21 September 2020, press release, https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers/.*

259. *Privacy International, 'Surveillance Disclosures Show Urgent Need for Reforms to EU Aid Programmes', 10 November 2020, https://www.privacyinternational.org/long-read/4291/surveillance-disclosures-show-urgent-need-reforms-eu-aid-programmes.*

260. *AP News, 'EU agrees on tighter rules for surveillance tech exports', 9 November 2020, https://apnews.com/article/global-trade-europe-d1d1d278bb5f34b2160dae2aad48c34d.*

261. *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), https://eur-lex.europa.eu/eli/reg/2021/821/oj.*

262. *Privacy International, 'Human Complaint on EU surveillance transfers to third countries', https://privacyinternational.org/legal-action/complaint-eu-surveillance-transfers-third-countries.*

263. *Privacy International, 'Human Rights Groups Submit Complaint to European Ombudsman Calling for Investigation into EU Surveillance Aid', 15 October 2021, https://privacyinternational.org/news-analysis/4652/human-rights-groups-submit-complaint-european-ombudsman-calling-investigation-eu.*

264. *See the introduction of the current study in relation to "Surveillance Study". See also David Lyon, Surveillance Studies: An overview, ed. Polity, 2007; Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, London, 2010; Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020; Olivier Aïm, Les théories de la Surveillance – Du panoptique aux Surveillance Studies, ed. Armand Colin, 2020.*

265. *François Sureau, Pour la liberté - Répondre au terrorise sans perdre la raison, Tallandier, essais, 2017. François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019.*

266. *United Nations High Commissioner for Human Rights, The right to privacy in the digital age, 15 September 2021, https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx. See also United Nations, 'Urgent action needed over artificial intelligence risks to human rights', 15 September 2021, https://news.un.org/en/story/2021/09/1099972.*

267. *European Parliament, Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), Committee on Civil Liberties, Justice and Home Affairs, Motion for a European Parliament Resolution, on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters,*

13 July 2021, § 26-27, https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html?.

268. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 2-3, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

269. 'Amnesty International and more than 170 organisations call for a ban on biometric surveillance', 7 June 2021, press release, https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/.

270. 'Amnesty International and more than 170 organisations call for a ban on biometric surveillance', already mentioned.

271. https://reclaimyourface.eu/.

272. AFP, 'Reconnaissance faciale: un groupe d'ONG attaque Clearview AI dans cinq pays européens', 27 May 2021, https://www.france24.com/fr/info-en-continu/20210527-reconnaissance-faciale-un-groupe-d-ong-attaque-clearview-ai-dans-cinq-pays-europ%C3%A9ens; Florian Reynaud, 'Reconnaissance faciale : une enquête demandée à la CNIL sur les pratiques de Clearview AI', 27 May 2021, https://www.lemonde.fr/pixels/article/2021/05/27/reconnaissance-faciale-une-enquete-demandee-a-la-cnil-sur-les-pratiques-de-clearview-ai_6081644_4408996.html.

273. See for instance the French Constitutional Council, Decision n° 2017-635 QPC of 9 June 2017, following a request before the Council of State raised by the association La Ligue des Droits de l'Homme [The League of Human Rights], https://www.conseil-constitutionnel.fr/en/decision/2017/2017635QPC.htm.

274. Statewatch, 'EU: Biometrics - from visas to passports to ID cards', https://www.statewatch.org/media/documents/analyses/no-49-eu-bio-passports-id-cards.pdf.

275. https://technopolice.fr/.

276. La Quadrature du Net, 'La Quadrature du Net ouvre la bataille contre la technopolice', 16 September 2019, https://www.laquadrature.net/2019/09/16/la-quadrature-du-net-ouvre-la-bataille-contre-la-technopolice/.

277. La Quadrature du Net, 'La Quadrature du Net ouvre la bataille contre la technopolice', already mentioned.

278. https://technopolice.be/.

279. Example of the training "Digital security for activists" that took place in Saint-Petersburg, Russia, on April 10, 2016: Ksenia Ermoshina and Francesca Musiani, 'Hiding from Whom? Threat-models and in-the-making encryption technologies', in Intermédialités: Histoire et théorie des arts, des lettres et des techniques / History and Theory of the Arts, Literature and Technologies, Erudit, 2018, Cacher/Concealing, 10.7202/1058473ar, halshs-02320706, p. 6, https://halshs.archives-ouvertes.fr/halshs-02320706/document. See also the Totem online learning platform, which focuses on digital security for human rights advocates (https://totem-project.org/).

280. See for example https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometric ; https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie

281. Ryan Mac, Caroline Haskins and Antonio Pequeño IV, 'Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here', 25 August 2021, BuzzFeed News, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

282. 'Trusted Cloud Principles signatories are committed to protecting the rights of our customers. We have agreed to strong principles that ensure we compete while maintaining consistent human rights standards', https://trustedcloudprinciples.com/.

283. Trusted Cloud Principles, https://trustedcloudprinciples.com/principles/.

284. David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p 191.

285. See subsections 7.1.3 and 7.3.3 of the current study.

286. 'La CNIL appelle à la tenue d'un débat démocratique sur les nouveaux usages des caméras vidéo', 19 December 2018, https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-video.

287. Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', Note du CREOGN, n° 43, September 2019, p. 4, https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-creogn/reconnaissance-faciale-et-controles-preventifs-sur-la-voie-publique-l-enjeu-de-l-acceptabilite.

288. Example of the protest, in Switzerland, against the new law introducing the biometric passport. This protest led to the organisation of a popular vote, which in turn resolved in favour of the new law (50,1 % of the votes cast were in favour of the passport): University of Basel, 'Case study: biometric passports', https://www.futurelearn.com/info/courses/switzerland-europe/0/steps/52460.

289. Noël Chahid-Nourai, in 'Secret et nouvelles technologies', colloque consacré au secret professionnel organisé par la Conférence des bâtonniers, Les petites affiches, n° 122, 20 June 2001, p. 25 s. See also, in the same line, Saskia Sasken, 'Politiques locales et réseaux mondiaux', in Revue des deux mondes, February 2001, p. 32.

290. Translated from French: Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 56. See also subsection 7.1.3 of the current study.

291. Linda Ravo and Jascha Galaski, 'Health of Our Democracies Compromised by Many EU Leaders During 2020: Liberties Report', 9 March 2021, https://www.liberties.eu/en/stories/demanding-on-democracy-liberties-report-2020/43366; Sarah Repucci and Amy Slipowitz, 'Democracy under Lockdown, The Impact of COVID-19 on the Global Struggle for Freedom', October 2020, Freedom House, esp. p. 4, https://freedomhouse.org/sites/default/files/2020-10/COVID-19_Special_Report_Final_.pdf. See also subsection 7.1.1.3 of the current study.

292. David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 167, referring to Gary T. Marx ('A tack in the shoe: Neutralizing and resisting

the new surveillance', in Journal of social issues, 59 (2), 2003, 369-90). Gary T. Marx refers to E. Goffman (Asylums, New-York: Penguin, 1961).

293. *The TOR project aims at preventing online tracking and surveillance: https://www.torproject.org/.*

294. *Such as Signal, Keybase, Element, and GnuPG. See Ksenia Ermoshina and Francesca Musiani, 'Hiding from Whom? Threat-models and in-the-making encryption technologies', in Intermédialités: Histoire et théorie des arts, des lettres et des techniques / History and Theory of the Arts, Literature and Technologies, Erudit, 2018, Cacher/Concealing, 10.7202/1058473ar, halshs-02320706, https://halshs.archives-ouvertes.fr/halshs-02320706/document.*

295. *Such as Veracrypt and Zed!.*

296. *David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 168, referring to Gary T. Marx ('A tack in the shoe: Neutralizing and resisting the new surveillance', in Journal of social issues, 59 (2), 2003, 369-90).*

297. *Fabien Soyez, 'Comment certains échappent aux caméras de surveillance et à la reconnaissance faciale', 21 January 2020 (update), https://www.cnetfrance.fr/news/comment-certains-echappent-aux-cameras-de-surveillance-et-a-la-reconnaissance-faciale-39897747.htm.*

298. *https://www.cryptoparty.in/. The website lists all local Crypto party initiatives around the world. Some of them have specific websites, such as the "Café Vie Privée" in France (https://café-vie-privée.fr/) and the Cryptoparty Heidelberg, in Germany (https://www.noname-ev.de/cryptoparty.html).*

299. *https://exodus-privacy.eu.org/en/.*

300. *Yale Law School, 'ISP Privacy Lab Publishes Research on Hidden Trackers', 28 November 2017, https://law.yale.edu/yls-today/news/isp-privacy-lab-publishes-research-hidden-trackers.*

301. *https://privacylab.yale.edu/about.html.*

302. *https://noyb.eu/en/our-detailed-concept.*

303. *See for example Andy Greenberg, 'How to Encrypt All of the Things', 12 September 2017, https://www.wired.com/story/encrypt-all-of-the-things/.*

304. *See for example https://www.privacytools.io/.*

4

THE LEGISLATION REGULATING SURVEILLANCE

4.1 THE ECHR AND THE EUCFR REQUIREMENTS

4.1.1 RESPECTING HUMAN RIGHTS AND THE RULE OF LAW: A SOCIETAL CHOICE IMPLYING MORE THAN FORMAL STATEMENTS

On 5 May 1949, the representatives of ten European countries[305] signed the Statute of the Council of Europe, the oldest European political organisation[306]. The aim was to establish an organisation capable of *"prevent[ing] a return to totalitarian regimes"*[307] through the defence of fundamental freedoms and the rule of law.

On 4 November 1950, the representatives of the Council of Europe member states[308] signed the European Convention on Human Rights (ECHR)[309], which was afterwards supplemented by additional protocols[310]. Nowadays, the ECHR in its version of 1 August 2021 is in force in the 47 Council of Europe member states[311], which include all the EU member states[312], and 7 additional protocols are in parallel open to signature and ratification[313].

The innovative character of the ECHR lies less in the list of the fundamental rights it establishes, which were derived from the UN Universal Declaration of Human Rights of 1948, than in the efforts made by its writers[314] both to specify the conditions under which these rights may be limited, and to set up a mechanism designed to ensure efficient and collective control of the enforcement of these rights.[315] Indeed, historical excesses had shown the inability of states to ensure the protection of human rights in the absence of counter-powers, because one of the state's main inherent characteristics is to *"seek efficiency"*[316] by *"giving precedence to order over freedom"*[317]. As a result, *"the Convention establishes objective obligations for states towards individuals, irrespective of the conduct of cosignatory states"*[318]. These obligations are enforced by national judges under the supervision of the European Court of Human Rights (ECtHR) as a last resort. The rulings of that Court are binding without possibility of appeal. They constitute a *"mandatory 'international public order' […] from which the states party to the Convention cannot derogate"*.[319]

In comparison, the EU Charter of Fundamental rights (EUCFR)[320] has a less binding scope. The Court of Justice of the European Union (CJEU), which is competent to judge on the violations of the EUCFR, is more difficult to access for European citizens. In addition, the CJEU supervision is limited to acts implementing EU law[321]. This being said, the CJEU makes its decisions in consideration of the requirements of both the EUCFR and ECHR, because the protection provided by the EUCFR is the same, in terms of meaning and scope, as that provided by the ECHR, in relation to rights enshrined in both texts[322]. These circumstances maintain the prominent position of the ECtHR in regard to protection of fundamental rights of individuals in Europe.

It appears of utmost importance to emphasise that the respect for the dynamics of fundamental rights protection established in the ECHR is the condition for maintaining liberal democracy as a form of government. In this context, liberal democracy is understood as *"a political system in which […] liberties are well protected and in which there exist autonomous spheres of civil society and private life, insulated from state control"*[323].

Indeed, the design of such dynamics has been based on the works of great thinkers[324] such as Beccaria[325] and Tocqueville[326], 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 as to not pit freedom against security[327], and that there can be no balance between the one and the other[328] - even though they do not exclude each other[329].

Security is neither a condition for freedom, nor the first amongst freedoms.[330] Security is a derogation from the principle of freedom. In other words, security is a purpose that may be invoked to justify certain limitations of freedom, under the following strict conditions. Firstly, limitations of freedoms must be provided for by a clear law that ensures foreseeability. Secondly, limitations of freedoms must pursue a legitimate and determined purpose, connected with a need, for society, which must be demonstrated. Thirdly, limitations of freedoms must be both efficient and reduced to the strict minimum to reach this purpose. This implies both the minimisation of impacts on fundamental rights and the setting up of a certain number of 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"*. 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 be seized by concerned individuals.[331]

Getting out of this path, all the terms of which are of utmost importance, implies taking a road that inexorably leads, at one point, to totalitarianism. Remaining deaf to this alert can only induce a denial of history, as also recently recalled by numerous specialists[332], including Professors Jean Duffar and Jacques Robert, the latter being also a former member of the French Constitutional Court: *"Thus, if due care is not taken, this would imperceptibly tend to dangerously set root, including in countries that we previously believed to be insulated from contagion, a diffuse totalitarianism which, letting […] citizens believe that they still enjoy a freedom yet become illusory, maintains voluntarily the latter in the unconsciousness of an independency […] which, one day, would be irreversible"*[333].

4.1.2 FUNDAMENTAL RIGHTS IMPACTED BY THE USE OF MASS SURVEILLANCE TECHNOLOGIES

The ECHR and the EUCFR establish several rights and freedoms that are at stake where surveillance technologies are in use. These rights are identified below, together with a description of their content, which will be used within the framework of the impact analysis.

1) THE RIGHT TO PRIVATE AND FAMILY LIFE

The definition of the right to respect for private and family life, also called *"right to private life"* or *"right to privacy"*[334], is the subject of much debate due to differences in the qualifications given by courts to limitations to private life. Indeed, there are two coexisting notions of private life. The first notion comes from a philosophical conception, and refers to the *"right to be left alone"*[335] and to the right to shape one's own life with minimal outside interference[336]. The second notion is a legal conception of privacy, which may be defined by the respect that is due to the rights and freedoms of others[337]. Privacy as protected by law may basically be seen as the philosophical conception of privacy, with which third parties have no right to interfere, because such interference would not be necessary and/or proportionate.[338] Differences in understanding privacy appear mainly to be due to the fact that, when a court establishes an absence of privacy infringemenst, in a particular case, it often prefers considering that the information at stake was not (legally speaking) private, rather than considering that the information was private but legitimately or legally accessed, processed, or published, based on compliance with the requirements for necessity and proportionality. This context feeds numerous attempts to classify what is legally protected as private and what is not, which is literally impossible since, by definition, private life will not be protected the same way depending on the third party who interferes with it. This does not mean that non-protected information, in some contexts, does not remain private in nature, since it may be protected in other contexts[339].

This being said, the ECtHR[340] and the CJEU[341] have identified at least the following elements of legally protected private life content. The right to private life includes the right *"to live privately, away from unwanted attention"*[342], which covers for example the protection of *"the home address"*[343]. It also includes *"personal development»*[344], whether in terms of personality or of *"personal autonomy"*[345], as well as the right *«to establish and develop relationships with other human beings»*[346] and *"the outside world"*[347], which amounts to the right to a *"private social life"*[348], which implies the absence of *"outside interference"*[349]. The right to private life also includes a right to physical and social identity[350], and a right to *"physical and psychological integrity"*[351], which embraces *"multiple aspects of the person's physical and social identity"*[352] and which is *"primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings"*.[353] Finally, the right to private life includes the rights to personal data protection[354], dignity, and self-determination[355], which will be further addressed below independently since they are considered to be transverse to other rights at stake.

This protection of personal activity extends to public contexts[356] and to *«professional and business activities»*[357]. Interactions with others are protected in all their forms, including correspondence[358] which covers letters[359], pager messages[360], professional correspondence[361], correspondence intercepted in the course of business or from business premises[362], telephone calls and conversations[363], including information relating to these calls such as their date or the number dialed[364], and electronic communications (including the right for an individual to control *«information derived from the monitoring of (his or her) personal Internet usage»*[365]).

2) THE RIGHT TO THE PROTECTION OF PERSONAL DATA

Personal data is protected under article 8 of the ECHR concerning the right to private life[366], and in the EUCFR as an autonomous right in its article 8. The ECHR defines the notion of personal data, by referring to the Council of Europe Convention n° 108 for the protection of individuals with regard to automatic processing of personal data[367], as *"any information relating to an identified or identifiable individual"*[368], even indirectly through, for example, a dynamic IP address[369]. Such data is protected insofar it relates to the *"private life"* of an individual, this notion being broadly understood[370].

In particular, personal data is protected against both storage and release, even towards public authorities[371], regardless of the subsequent use of the information[372] and no matter the sensitive nature of the information. As a result, the storing of any personal information in a public authority database constitutes and interference per se[373], which must be necessary and proportionate in order to not be deemed arbitrary. Protected data includes information about the political activity of an individual[374] and health data[375]. Publicly accessible information is also protected[376], even though *"secret surveillance methods"* are not used[377], by virtue of a *"right to a form of informational self-determination, as regards data which, albeit neutral, are collected, processed and disseminated collectively"*[378]. As a result, the legal protection covers the *"systematic or permanent record"* of information coming from the public domain, and therefore the *"files gathered [that way] by security services on a particular individual"*.[379] An interference with private life is also found where photographs taken by the police in a public place aim *"to identify the persons photographed […] by means of data processing"*[380].

Personal data is moreover particularly protected within the context of *"surveillance methods resulting in masses of data collected"*[381] and, more generally, *"mere storing of information"*[382]. For example, an interference with private life is constituted by the GPS surveillance of an applicant by investigation authorities, leading to the systematic collection and storage of data determining *"the applicant's whereabouts and movements in the public sphere"*, as well as the recording and further use of these data *"in order to draw up a pattern of the applicant's movements, to make further investigations and to collect additional evidence at the places the applicant had travelled to"*[383].

According to the ECtHR, *"other methods of visual or acoustical surveillance"* are even more susceptible than GPS surveillance *"of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings"*[384]. Fingerprints[385], photographs, and voice samples also *"give rise […] to important private-life concerns"* when they are recorded *"in connection with an identified or identifiable individual"*, because they *"objectively contain unique information about the individual concerned, allowing his or*

her identification with precision in a wide range of circumstances".[386] For example, *"the recording, by the police, of applicants' voices when [they were] being charged and when [they were] in their police cells"*[387] was found to be an interference with the right to private life.

3) THE RIGHT TO FREEDOM OF EXPRESSION

The right to freedom of expression is protected both at the Council of Europe[388] and EU[389] levels. This right includes the *"freedom to hold opinions and to receive and impart information and ideas without interference [...] and regardless of frontiers"*[390], which means that it includes a right of communication of individuals between themselves[391], and a corresponding right to receive information[392], especially where the information is of public interest[393].

The right to freedom of information is moreover *"applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the state or any sector of the population"*[394]. The ECtHR explains that *"such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'"*[395].

In parallel, freedom of expression *"carries with it duties and responsibilities"*[396] for the author and the recipients of an information, which are linked to the respect that everyone must show for the rights and interests of others[397]. Information recipients have the duty to tolerate contrary opinions and to accept constructive criticism (without which there can be no intellectual debate).[398] The person who expresses an idea should do it with restraint, avoiding forward 399. Moreover, embodying an idea with tact and courtesy does not prevent the defence of that idea, while a respectful tone and chosen words generally benefit this defence[400].

The organs of the Council of Europe[401] regularly affirm that these requirements condition both:

• The respect of each individual as a person, since their thoughts, opinions and beliefs are an integral part of their identity[402]. In that sense, respecting the conditions for exercise of the freedom of expression is a condition for «*the development of every [human being]*»[403].

• A constructive exchange of ideas and opinions, which are essential both to the holding of a public debate[404] and to creativity, the search for the truth and cohesion[405].

In that sense, the ECtHR evokes freedom of expression as an *"essential foundation"*[406] of democracy and the rule of law and *"one of the basic conditions for its progress"*[407]. This approach is also the approach adopted by the EU, which can be summarised by quoting the EU Parliament: *"freedom of expression in the public sphere has been shown to be formative of democracy and the rule of law itself, and coaxial to its existence and survival"*[408].

As a consequence, states have a positive obligation to ensure the effectiveness of these rights, which implies giving citizens the confidence that they can express themselves without fear[409], to enable them to reply to published information[410] and to give them the skills and critical attitude enabling them to face and understand the information they receive, including where this information is harmful to them. Citizens' education and awareness must include the ability to distinguish between true and false information, to understand the benefits and risks of measures aiming at regulating speeches and content, and to have a democratic and responsible attitude that respects the rights of others. This right of education is of particular importance and has been especially highlighted in several recommendations by the Council of Europe Committee of Ministers[411] as well as by the European Parliament[412].

Finally, the right to freedom of expression also includes a right to access the Internet and a right to freedom of media. Member states must especially *"foster as much as possible a variety of media and a plurality of information sources, thereby allowing a plurality of ideas and opinions"*[413]. This requirement of pluralism of media, which gives consistency to the freedom to be informed, is also expressly mentioned in the EU Charter of Fundamental Rights in Article 11, 2414.

4) THE RIGHT TO FREEDOM OF ASSEMBLY AND ASSOCIATION

The right to freedom of assembly and association is protected both at the Council of Europe[415] and EU[416] levels. This right *"constitutes an individual right that is exercised collectively"*[417]. It protects *"the non-violent gathering of a number of people in a*

publicly accessible place with a common expressive purpose"[418]. This means that it *"assumes that an assembly is for the purpose of conveying a message [which] might be aimed at an individual, a group, an organisation or at society in general"*[419].

Freedom of assembly *"includes public or private meetings, marches, processions, demonstrations and sit-ins. The purpose may be political, religious or spiritual, social or another purpose; no limit has been imposed on purpose, but any assembly must be peaceful. Incidental violence will not mean an assembly forfeits protection unless it had a disruptive purpose"*[420]. The right to freedom of assembly covers not also the right to organise and participate in assemblies but also other activities such as the observation, monitoring or recording of them[421].

Some assemblies might moreover *"create unpredictable situations for the authorities"* and *"may cause some level of temporary interference with, or disruption of, routine daily activities"*[422]. In such case, the rights to routine and to assembly must be balanced, because the second one is an *"important element of life in a democratic society"* and it carries *"as much right to the use of public spaces as people involved in other activities"*.

According to the Council of Europe Committee of Ministers, freedom of assembly also implies that *"individuals are free to use Internet platforms, such as social media and other ICTs in order to associate with each other and to establish associations, to determine the objectives of such associations, to form trade unions, and to carry out activities within the limits provided for by laws that comply with international standards"*[423]. Indeed, *"ICTs bring an additional dimension to the exercise of freedom of assembly and association, [which] has crucial implications for the strengthening of civil society […] and for the democratic process in general"*[424]. For this purpose, the Council of Europe Committee of Ministers recommends that member states *"adapt their legal frameworks to guarantee freedom of ICT-assisted assembly and take the steps necessary to ensure that monitoring and surveillance of assembly and association in a digital environment does not take place, and that any exceptions to this must comply with those provided for in Article 11, paragraph 2, of the ECHR"*[425].

5) THE RIGHT TO FREEDOM OF OPINION

The right to freedom of *"thought, conscience and religion"* is protected both in the ECHR and in the EUCFR[426]. It includes the right to hold a belief and the right to manifest that belief. The right to hold a belief *"is absolute and unconditional"* which means that the *"state cannot interfere with it for instance by dictating what a person believes or taking coercive steps to make him change his beliefs"*.[427]

The right to manifest one's beliefs alone or with others, in private or in public, is for its part not absolute and might be limited provided that the requirements analysed in subsection 4.1.3 of the current study are respected[428]. The manifestation of an opinion might take several forms but there must be *"a sufficiently close and direct nexus between the act and the underlying belief"* to call for the protection of the related freedom.[429] Finally, if the ECtHR accepts the possibility for states to question *"the sincerity of an individual's alleged religion in exceptional cases"*, the general rule is that they *"are not justified in casting doubt on the sincerity of the beliefs which an individual claims to hold without supporting their position with solid, cogent evidence"*.[430]

6) THE RIGHT TO FREEDOM OF MOVEMENT

Freedom of movement is protected in the EUCFR and by Protocol n° 4 to the ECHR, which has not been ratified by all EU members[431].

This right includes the right of citizens and other people that are lawfully within the territory of a given state, to move and to freely choose their residence within this territory, as well as to leave it. For example, interferes with the freedom of movement the *"requirement to report any change of place of residence […] or to have it registered by the police within a specific time-limit, on pain of a fine"*, *"an inability to enter a specified area of a city, or a prohibition thereof"* and *"extensive police monitoring of movements between a territorial entity not recognised by the international community and a government-controlled area and within the latter, coupled with the requirement to report to the police before each intended border crossing"*.[432] On the opposite, the possibility of being stopped and searched by the police in a security risk area,

designated such *"in response to a rise in violent crime"*, even though this possibility generates a fear to be subjected to such control, does not constitute a limitation of the freedom of movement since individuals are *"in no way prevented from entering that area, moving within it and leaving it again"*.[433]

7) THE RIGHT TO LIBERTY AND SECURITY

The right to liberty and security, established in the ECHR and the EUCFR[434], relates to the *"physical liberty"* of a person, with the aim of ensuring that no one is *"deprived of that liberty in an arbitrary fashion"*.[435]

Even measures intended for protection or taken in the interest of the person concerned may be regarded as a deprivation of liberty.[436] The notion of deprivation of liberty *"contains both an objective element of a person's confinement in a particular restricted space for a not negligible length of time, and an additional subjective element in that the person has not validly consented to the confinement in question"*[437]. *"Relevant objective factors to be considered include the possibility to leave the restricted area, the degree of supervision and control over the person's movements, the extent of isolation and the availability of social contacts"*[438]. Deprivation of liberty might be established even if the length of the detention is *"relatively short"*[439], and even in this circumstance, *"an element of coercion in the exercise of police powers of stop and search is indicative of a deprivation of liberty"*[440].

8) THE RIGHT TO NON-DISCRIMINATION PROHIBITION OF DISCRIMINATION

The prohibition of discrimination is established in article 21 of the EUCFR, in article 14 of the ECHR and in article 1 of the Protocol n° 12 to the ECHR[441]. The EUCFR and Protocol n° 12 to the ECHR provide *"for a general prohibition of discrimination"*, while the protection provided in article 14 of the ECHR is limited to a prohibition of discrimination *"in the enjoyment of one or the other rights guaranteed by the Convention"*[442]. This being said, there is a relative autonomy of article 14 of the ECHR, because it does not *"necessarily presuppose the violation of one of the substantive rights guaranteed by the Convention"*[443]. As a result, the existence of a link between discrimination and a right protected in the ECHR is sufficient to claim protection of article 14 of the ECHR.

Thin differences between texts also exist in relation to the grounds on which discrimination is prohibited. All texts prohibit discrimination based on *"any ground such as"* sex, race or ethnic origin, colour, language, religion, political or other opinion, membership (EUCFR) or association (ECHR) with a national minority, property, and birth. The EUCFR adds *"disability, age or sexual orientation"*, whereas the ECHR and its protocol add *"other status"*. This latter notion also covers disability, age, or sexual orientation, in addition to gender identity, parental and marital status, status related to employment, as well as a complementary series of grounds.[444]

In relation to the content of the protection, article 14 of the ECHR protects against direct and indirect discrimination as well as discrimination by association, and the ECtHR may bring such a violation directly into the debates, even though the applicant did not invoked this violation in his or her claim[445]. The notion of direct discrimination *"describes a difference in treatment of persons in analogous, or relevantly similar situations"* and *"based on an identifiable characteristic, or 'status'"*.[446] For example, *"harassment and instruction to discriminate can be seen as particular manifestations of direct discrimination"*[447]. Indirect discrimination *"may take the form of disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, has a particular discriminatory effect on a particular group"* and *"although the policy or measure at stake may not be specifically aimed or directed at a particular group, it might nevertheless discriminate against that group in an indirect way"*.[448] In addition, *"indirect discrimination does not necessarily require a discriminatory intent"* and it *"may arise [either] from a neutral rule […] or from a de facto situation"*.[449] Discrimination by association, for its part, arises in *"situations where the protected ground in question relates to another person somehow connected to the applicant"*.[450]

Finally, we can highlight that Article 14 of the ECHR does *"not prohibit a member state from treating groups differently in order to correct 'factual inequalities' between them; indeed in certain circumstances, failure to attempt to correct such inequality through different treatment may in itself give rise to a breach of article 14"*.[451]

9) THE RIGHT TO EDUCATION

The right to education is established in article 2 of protocol n° 9 to the ECHR[452] and in article 14 of the EUCFR. It includes the right to education and to have access to vocational and continuous training[453] as well as the right of parents to ensure the education and teaching of their children in conformity with their religious and philosophical convictions. Article 14.2 of the EUCFR adds *"the possibility to receive free compulsory education"*. This principle *"merely implies that […] each child has the possibility of attending an establishment which offers free education. It does not require all [educational] establishments […] to be free of charge. Nor does it exclude certain specific forms of education having to be paid for, if the state takes measures to grant financial compensation"*[454].

The ECtHR considers that *"in a democratic society, the right to education, which is indispensable to the furtherance of human rights, plays such a fundamental role"* that it must not be interpreted restrictively.[455] In addition, this right must be read in conjunction with other rights enshrined in the ECHR and its protocols such as the right to private life, *"including the concept of personal autonomy"*, the right to freedom of thought and *"to receive and impart information and ideas"*, and the prohibition of discrimination.[456]

According to the ECtHR, this right *"must be interpreted in harmony with other rules of international law of which the Convention forms part"*, for example the Universal Declaration of Human Rights (1948), the UN Convention on the Rights of the Child (1989), and the revised European Social Charter.[457] This right *"covers a right of access to educational institutions existing at a given time […], transmission of knowledge and intellectual development [and] the possibility of drawing profit from the education received"* such as *"official recognition of the studies which have been completed"*.[458]

10) THE RIGHT TO A FAIR TRIAL AND RELATED RIGHTS

The right to an effective remedy and to fair trial includes several sub-rights. First in line are the right to access to a court and the right to benefit from several institutional and procedural guarantees (tribunal established by law, independent and impartial; fairness, equality of arms and adversarial proceedings; reasoning of judicial decisions; right to remain silent and to not incriminate oneself; use of evidence obtained lawfully; right to a public hearing and to be judged within a reasonable timeframe). Other guarantees are of a more substantial nature and cover the presumption of innocence and the rights of the defence[459], as well as the principles of legality and proportionality for criminal offences. All these sub-rights are protected in articles 47 to 50 of the EUCFR and in articles 6, 7 and 13 of the ECHR. Moreover, the Council of Europe Committee of Ministers recalled that the rights to a fair trial and to the presumption of innocence *"should be respected in the digital environment"*[460]

According to the ECtHR, the principle of the presumption of innocence *"requires, inter alia, that: (1) when carrying out their duties, the members of a court should not start with the preconceived idea that the accused has committed the offence charged; (2) the burden of proof is on the prosecution, and any doubt should benefit the accused"*[461]. It is also *"to prosecution to inform the accused of the case that will be made against him or her, so that he or she may prepare and present his or her defence accordingly, and to adduce evidence sufficient to convict him or her"*[462]. However, *"presumptions of fact or of law"*, which *"operate in every criminal-law system [are] not prohibited in principle by the Convention"*[463].

This principle is applicable in the context of *"criminal charges"*, but the notion of *"crime"* is autonomous under the jurisprudence of the ECtHR, and therefore *"independent of the categorisations employed by the national legal systems of the member states"*[464]. This means that the ECtHR may consider that a limitation of any given right, established in a state, is a criminal penalty, even though it has not this very qualification in the concerned state. In order to determine the criminal nature of the proceeding, the ECtHR retains a set of criteria, which are not necessarily cumulative and which are the classification in domestic law, the nature of the offence and the severity of the penalty to which the person concerned is exposed.[465]

The principle of legality of penal offences, according to which *"only the law can define a crime and prescribe a penalty"*[466] (which implies the principle of non-retroactivity of criminal law, except for lighter penalties[467]), applies to the autonomous notion of *"criminal area"* as it has been defined in relation to the right to presumption of innocence[468]. The concept of *"law"* is in addition understood broadly, as in the other ECHR provisions, and covers *"both domestic legislation and case-law, and comprises qualitative*

requirements, notably those of accessibility and foreseeability"[469]. The concept of penalty also has an autonomous scope and the ECtHR is *"free to go beyond appearances"*. It *"autonomously assess[es] whether a specific measure is, substantively, a 'penalty' within the meaning of Article 7 1. The starting point for any assessment […] is to ascertain whether the measure in question was ordered following a conviction for a 'criminal offence'"*.[470] *"Other factors may be deemed relevant in this respect: the nature and aim of the measure in question (particularly its punitive aim), its classification under domestic law, the procedures linked to its adoption and execution and its severity […]. However, the severity of the measure is not decisive in itself, because many non-criminal measures of a preventive nature can have a substantial impact on the person concerned"*[471].

According to the Council of Europe Committee of Ministers, and such as the right to a fair trial, *"the right of no punishment without law applies equally to a digital and a non-digital environment"*[472].

11) THE RIGHT TO DIGNITY AND TO SELF-DETERMINATION

The right to dignity is established in article 1 of the EUCFR. It is not subject to a dedicated provision in the ECHR, but the ECtHR considers that *"the very essence of the Convention is respect for human dignity and human freedom"*[473]. The reading of the ECtHR decisions suggests that the principle of dignity protects the intimacy of individuals in relation to their body and their mind – and further their human personality as such, as if there was, around the individual, a zone of intimacy that states and third parties can never cross.

In relation to the body of individuals, the ECtHR protects inter alia[474] human dignity under the right to life[475] and the prohibition of torture and degrading treatment[476]. Within the framework of the protection of these rights, the violation of dignity appears to happen where a treatment, applied to an individual, results from the use of a disproportionate force – assessed contextually in compliance with the proportionality assessment rules[477] - without the individual's consent. For example, *"where an individual is confronted with law-enforcement officers, any recourse to physical force which has not been made strictly necessary by the person's conduct diminishes human dignity"*[478]. It is also a violation of human dignity to impose a *"medical treatment without the consent of a mentally competent adult patient"*[479] or to collect such consent in a way that the consent was not freely given, because it was not fully informed and was requested at a moment where the person concerned was not mentally available[480]. The violation of human dignity, and further of the right to not be subjected to a degrading treatment, may be established although no intention of ill-treatment was established[481].

The Council of Europe Convention on Human Rights and Biomedicine[482] also affirms in its preamble the *"importance of ensuring the dignity of the human being"* which might be endangered by *"the misuse of biology"*, together with the resolution of its writers *"to take such measures as are necessary to safeguard human dignity and the fundamental rights and freedoms of the individual with regard to the application of biology […]"*. Article 1 of the Convention requires member states to *"protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology […]"* and to take in their internal law *"the necessary measures to give effect"* to the provisions of the Convention. Article 2 affirms the *"primacy of the human being"* and clarifies that *"the interests and welfare of the human being shall prevail over the sole interest of society or science"*. Finally, article 28 of the Convention requires states to *"see to it that the fundamental questions raised by the developments of biology and medicine are the subject of appropriate public discussion in the light, in particular, of relevant medical, social, economic, ethical and legal implications, and that their possible application is made the subject of appropriate consultation"*.

In relation to the mind and human personality of individuals, respect for human dignity is ensured within the framework of the protection of the right to a fair trial, for example by ensuring that *"all elements which [are] favourable to the defendant's legal position [are] brought before the court"*[483]. It is also ensured within the framework of the protection of freedom of expression, which must be balanced with *"interests relating to the protection of the honour and dignity of others"*[484]. It is also ensured within the framework of the prohibition of discrimination. For example, inappropriate conduct of police officers during a search, *"motivated by homophobic and/or transphobic hatred"* and arousing *"the applicants feelings of fear, anguish and insecurity [is] not compatible with respect for [applicants'] human*

dignity"[485]. Such discrimination may in addition be considered as degrading treatment that violates the prohibition of torture, which is not *"limited to acts of physical ill-treatment [but] also covers the infliction of psychological suffering […] if it humiliates or debases an individual in the victim's own eyes and/or in other people's eyes, whether or not that was the aim, if it breaks the person's physical or moral resistance or drives him or her to act against his or her will or conscience, or if it shows a lack of respect for, or diminishes, human dignity"*[486].

Respect for human dignity is moreover ensured as a component of the right to private life, covering for example *"offensive and vulgar"* statements on a Facebook page[487] and the possibility, for a disabled person, to see their *"will and preferences […] respected […] in respect of their family relationships and their right to choose their place of residence"*. This is because this freedom of choice is *"an inherent part of a person's autonomy, independence, dignity and self-development"*[488].

The latter decision is of particular interest, read in conjunction with the other decisions of the Court, and particularly the protection it offers to dignity through the prohibition of imposing a medical treatment without the free and fully informed consent of the patient[489]. Indeed, human dignity appears to imply the prohibition of any *"paternalistic 'best interests' decision-making"* that would *"overrid[e] or ignor[e]"* the *"will and preference of persons"* who are in a position to give their opinion[490], the state having the duty[491] to ensure that the best contextual parameters are set up in order to enable such opinion to be issued. This is in line with the duty of states to ensure that *"the fundamental questions raised by the developments of biology […] are the subject of appropriate public discussion in the light, in particular, of relevant medical, social, economic, ethical and legal implications, and that their possible application is made the subject of appropriate consultation"*[492].

Respect for this sphere of dignity, that surrounds an individual, does not suffer any exception. Indeed, an exception would drive to the suppression of the fundamental right that is limited *"in an undignified manner"*, and suppressions of rights are prohibited by the ECtHR[493]. Some authors refer to the *"essence/substance/core"* of fundamental rights, which *"should be respected under any circumstances, [because] its infringement should be unjustifiable: It constitutes the "*limit to the limits*".*[494] *In that sense, the use of the principle of dignity, by the Court, is an explicit "*signal to states on the importance of what is at stake*"*[495] and cannot suffer any interference.

This is in line with the approach that views *"human dignity as the foundation of human rights"*[496], since it conditions the existence of these rights. This is also in line with the approach that considers the right to private life[497] as a *"'fundamentally fundamental right'"* which necessarily preconditions, together with the right to personal data protection[498], *"the enjoyment of most other fundamental rights and freedoms"*[499]. Indeed, human dignity implies the possibility to make free choices, and therefore implies the existence of a right to self-determination. The right to self-determination implies, in turn, the respect of a zone of confidentiality[500], which may condition the making of certain choices[501]. For this reason, the right to self-determination is mainly protected, by the ECtHR, under the right to private life[502].

As a consequence, the right to privacy protects dignity, through the protection of a zone of confidentiality and of self-determination, with which no interference is allowed, neither from states nor from third parties.

This conclusion leads to another, already drawn up by Dr. Antoinette Rouvroy and Professor Yves Poullet, according to whom the right to privacy, through the right to self-development, *"is not conceived as the liberty held in isolation by an individual living secluded from the rest of society, but, on the contrary, as a right enjoyed as member of a free society"*[503]. In that sense, the right to self-determination – and therefore the right to privacy - may be considered *"as a tool for guaranteeing the democratic functioning of society"*[504] since it is *"a precondition to real democratic discussion"*[505].

The authors refer to a decision of the German Supreme Court from 1983, which declared unconstitutional certain provisions of a law that was granting the government with powers in terms of personal data collection for statistical purposes[506]. Ruling on the principle of dignity and the principle of self-development, which are both enshrined in the German Constitution[507], the Supreme Court stated that processing possibilities, including unlimited storage and retrieval capabilities as well as creation of profiles through databases interconnections, undermine the dignity and right to self-development of individuals where these persons have *"no sufficient means of controlling its truth and*

application" which lead to possibilities *"of inspection and of gaining influence"* which may *"influence the individual's behaviour by the psychological pressure exerted by public interests"*, which in turns impacts the individual's *"chances of development"* and *"the common good ("*Gemeinwohl*"), because self-determination is an elementary functional condition of a free democratic society based on its citizens' capacity to act and to cooperate"*[508]. In the same line, *"those who count with the possibility that their presence at a meeting or participation in a civil initiation be registered by the authority will be incited to give up practising their basic rights (Basic Law, Art. 8 . 9)"*[509].

Thus, the right to privacy, through the right to self-development, is not only a private *"right to be left alone"*[510] and a right that encloses or is at least strongly interlinked with the right to data protection[511], but also a right whose exercise is eminently public: through the preservation of fundamental freedoms and their impassable threshold of dignity and self-determination, the right to privacy enables human beings to be themselves, *"to develop and exercise their moral powers"*[512], and therefore to truly exchange with their counterparts. The *"freedom of political debate [being] at the very core of the concept of a democratic society"*[513], the right to privacy therefore *"guarant[ees] the democratic functioning of society"*[514] by empowering *"citizens to participate in the political system"*[515].[516]

This prohibits - citing and complementing the wording of the ECtHR - any *"paternalistic 'best interests' decision-making"* that would *"overrid[e] or ignor[e]"* the *"will and preference of persons"*[517] who are in a position to give their opinion. This will and preference may also refer to the collective choice of citizens in relation to the values that society must protect, and in relation to the means used in order to enforce such values[518]. In addition, the state has the duty to ensure that the best contextual parameters are set up in order to enable such opinion to be issued, through the organisation of an effective public debate where it is necessary[519]. This conclusion is consistent with the statement from the European Commission, according to which *"the right to human dignity is an inviolable right that requires every individual to be treated with respect as a human being and not as a mere 'object' and their personal autonomy respected"*[520].

It is when this zone of dignity is flouted, leading to the suppression of some freedoms including the right to privacy, despite the guarantees that have been foreseen in the ECHR and the EUCFR, that the right to resist oppression applies.

12) THE RIGHT TO RESIST OPPRESSION

The right to resist oppression, in the meaning of resistance to a tyrannical regime, does not appear in the ECHR and in the EUCFR, nor in most other international treaties[521], whereas it is not uncommon in national Constitutions[522]. This seems to be a consequence of the fact that these treaties organise a system in which such a right does not have a proper place.

Indeed, the European Convention on Human Rights organises the protection of fundamental rights, which are supposed to be enforced by domestic courts under its supervision in last resort[523]. In addition, the preamble of the Convention engages states to ensure *"an effective political democracy"* as the best instrument to maintain fundamental freedoms. Therefore, the right to resist oppression applies where democracy and judicial remedies are not effective. In other words, it applies when the Convention is not respected at its foundations – and further not applicable anymore based on the choice, implicit or explicit, of a state. As an author stated, *"it is difficult to imagine that the law may establish a rule that might contribute to weaken its very foundations"*[524], or that might result in an admission of failure of the fundamental rights protection mechanisms it established[525].

This being said, several authors identify a right of resistance to oppression as a general principle of international law[526], based on a *"right to democracy"*, being itself an *"internal component"* of a right to self-determination[527] which is read in the UN Universal Declaration of Human Rights of 1948528. This appears absolutely consistent with the principles of dignity and of self-determination that are protected against any interference by the ECtHR[529], since the UN Universal Declaration of Human Rights of 1948 inspired the writers of the ECHR[530], which itself refers to the Declaration in its Preamble. This is also in line with authors, such as Paul De Hert and Serge Gutwirth, who base the right to resist oppression on the right to privacy, which in turns guarantees the *"freedom to self-determination"* and *"each person's uniqueness, including alternative behaviour and the resistance to power at a time when it clashes with other interests or with the public interest"*[531]

4.1.3 THE CONDITIONS FOR LIMITING FUNDAMENTAL RIGHTS IN A DEMOCRATIC SOCIETY GOVERNED BY THE RULE OF LAW

Rights and freedoms enshrined in the ECHR and the EUCFR are of two kinds. Some of them are called *"absolute"*, because they cannot suffer any limitation, such as the right to hold a belief[532]. The other rights and freedoms are deemed *"conditional"*[533], because they can be limited following strict conditions, which most of the time lie in a general rule, sometimes called *"public order clause"*[534]. This general rule[535] or *"public order clause"*, which must be interpreted in a restrictive way[536], is provided in the ECHR and was further clarified by the ECtHR. It establishes that any limitation of a fundamental right (we can also say *"interference with a fundamental right"*) must have a specific, clear, accessible and foreseeable legal basis, must have a legitimate aim[537] and must be necessary and proportionate to achieve that aim[538].

This previous legal statement is often designated under four principles which are the principles of legal basis, legitimate purposes, necessity and proportionality. These four principles constitute general principles of the Union's law[539] and are therefore very often recalled in the European legal instruments, and, sometimes with a few variations, reflected in national laws. In addition, they influence national constitutional courts such as the French Constitutional Council[540] and the Romanian Constitutional Court[541]. Since the Treaty of Lisbon came into force, these four principles have also been fully integrated within the European Union law, based on Article 52, 1 of the EU Charter of Fundamental Rights.

These four principles may be summarised in two principles, namely the requirements for necessity and proportionality. Indeed, these two latter requirements already include the requirements for legitimate aim and for legal basis, which were established in addition as autonomous principles, given their importance. The principles of necessity and proportionality so defined are mandatory for the Council of Europe and the European Union member states, which must refrain from violating them, must be able to demonstrate their respect[542], and also have a positive obligation to take the measures necessary for these principles to be enforced between the individuals themselves[543].

The requirements for necessity and proportionality, which we detail below, are composed of four sub-requirements. A limitation of freedom must have a determined and legitimate purpose, must be efficient and reduced to the strict minimum in terms of impacts, and must be framed by a set of guarantees designed to prevent arbitrariness.

1) THE REQUIREMENT FOR A DETERMINED AND LEGITIMATE PURPOSE

The principle of necessity basically consists in the demonstration that any interference with a fundamental right must be appropriate to satisfy a specific social need. The first requirement included in the latter sentence is therefore that a specific and determined purpose motivate the interference.

This purpose must be designed to answer a *"pressing social need»*. This refers to a social issue that needs to be addressed[544]. This need must be determined and convincingly established[545] *«within the broader sphere of the legitimate aim pursued»*[546]. The latter legitimate aim must itself be enclosed in the list that is provided in relation to each of the fundamental rights established in the ECHR, which are, in relation to most fundamental rights, *"the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others"*[547]. The expression used in the EUCFR is wider since it refers to *«objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others»*[548].

This need which motivates the interference, must be *«pressing»*. In other words, it must have a certain *«level of severity, urgency or immediacy»*[549]. In relation to the state's actions, harm may result on society if the need is not addressed, taking into account the views of society and potentially divergent opinions regarding this particular *«need»*[550]. It must also be immutable and not extensible, since the other requirements will be assessed in its light[551]. Consequently, any change in - or extension of – purposes must lead to a new assessment of the necessity and proportionality of the interference that results from this change.

2) THE REQUIREMENT FOR EFFICIENCY

The limitation that is brought to a fundamental right must be appropriate to satisfy the purpose of this limitation[552]. This means that it may effectively mitigate the harm caused to society[553], and this *"must be supported by sufficient evidence"*[554] as clarified by the European Data Protection Supervisor. This classical position of the ECtHR[555] was also recalled by the Article 29 Data Protection Working Party in several opinions, notably relating to the application of the principles of necessity and proportionality within the law enforcement sector[556] and in relation to the retention of Internet traffic data[557].

Both the Article 29 working group and the ECtHR also clarified that the analysis of the effectiveness of a limitation of fundamental rights implies the review of a certain number of contextual elements. This especially includes reviewing *«the effectiveness of existing measures»* that aim to address the same objective. These existing measures need to be reviewed *«over and above the proposed measure»*, and an explanation must justify why they *«are no longer sufficient»*, and how the proposed measure will bring remedies[558].

3) THE REQUIREMENT FOR MINIMISATION

The requirement for minimisation is the first of the two main principles forming the principle of proportionality, which is *"recognised as one of the central principles governing the application of the rights and freedoms"* contained in the ECHR and its additional Protocols.[559] Indeed, it allows *"some evaluation of how much of a contribution a particular restriction can make towards securing a given objective"*[560]. Consequently, it satisfies *«the need for balancing entailed when giving effect to the rights"* protected under the ECHR. Without the proportionality requirement, *"the formulation of Convention provisions would be open to restrictions depriving the rights and freedoms of all content so long as they were prescribed by law and for a legitimate purpose"*[561], in addition to answering a *"pressing"* particular need.

The requirement for minimisation is also often referred to as a principle of *"strict necessity"* of the interference. It implies that a given interference with a fundamental right does not go *«further than needed to fulfil the legitimate aim being pursued»*[562]. In relation to public authority surveillance, this further implies that the interference is *"strictly necessary, as a general consideration, for the safeguarding of the democratic institutions and, moreover, [...] strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation"*[563].

The principle of minimisation implies both that the impacts of the interference be reduced to the minimum possible and that, once this minimisation has taken place, the remaining impacts not exceed the benefits of the interference for society[564]. In order to reach these requirements, a different set of questions needs to be considered. These questions are related to the content, the extent, and the nature of the measure causing an interference with freedoms.

Firstly, the interference must be adapted to its context[565], which notably implies taking into account several elements such as the severity of the need motivating the interference, and the legitimacy of the right which is limited.

Where the purpose is linked to public security and prevention or detection of crime, the severity of the need must be assessed having regards to the specific crime the measure is intended to address, and to the harm that crime would cause to society if not addressed[566].

The legitimacy of the right that is affected[567] may be assessed through the identification of the fundamental rights that base the behaviour which is limited (e. g. private life or freedom of expression), of the sensitivity of the data that may be collected, of the high or low expectations, in terms of confidentiality, of the individuals whose fundamental rights will be restricted[568], and of these individuals' characteristics, such as their age and their adaptation capabilities[569].

Secondly, the scope of the interference must not exceed what is necessary to reach the aim pursued[570]. This notably requires limiting, to the greatest extent possible, the volume of the intrusions into privacy, as well as the number of personal information collected. This also requires limiting, to the greatest extent possible, the number of places and of people affected[571], the cases of exercise of the measure (the powers of decision and action of law enforcement agencies must especially

be limited to what is strictly necessary), and the time during which the measure will be effective[572].

Thirdly, regarding the nature of the interference, the ECtHR verifies if the aim of the interference *"can be satisfactorily addressed in some other, less restrictive way"*[573]. For instance, *"an order requiring a journalist to disclose his source for a leak about the financial affairs of a company was considered to be unjustified […] insofar as the objective was to prevent dissemination of confidential information"*. Indeed, *"this legitimate concern was already being secured by an injunction restraining publication of the information that had been disclosed"*[574]. Consequently, the ECtHR considers that *«an explanation of what other measures were considered and whether or not these were found to be more or less privacy-intrusive"* should have been presented, and *"if any were rejected which were found to be less privacy-intrusive, then the strong justifying reasons as to why this measure was not the one that was selected to be implemented should [have been] given»*[575].

4) THE REQUIREMENT TO SET-UP GUARANTEES

Limitations of fundamental rights must be constrained by appropriate guarantees or safeguards, which must be *"adequate and effective"*[576].

A first set of guarantees, which we can call *"palliative"* or *"corrective"* measures, aims to palliate potential weaknesses that were found during the necessity and proportionality tests[577] in relation to purposes, efficiency and minimisation. This, in particular where technology used does not itself make it possible to restrict the scope and the extent of the limitation of freedoms. For example, in case the use of a given technology implies collecting more information than needed to fulfil a given objective, a *"palliative"* or *"corrective"* measure might be to obtain the consent of data subjects, or to shortly anonymise unnecessary information under independent supervision.

A second set of guarantees must be implemented in order to *"render possible"*[578] the actual respect for the results of the necessity and proportionality test, including the corrective measures that enabled successful completion of the test. The most important of these guarantees is the setting-up of what might be called a *"constraining transparency"*, which has been established as the autonomous principle of legal basis in the ECHR and ECtHR court cases[579]. Other guarantees might be of a legal, organisational[580] or technical nature[581].

A. CONSTRAINING TRANSPARENCY, BASED ON LAW

Transparency must be implemented in relation to any limitation of fundamental rights, so as to ensure accessibility and foreseeability towards the people concerned, and a corresponding binding force for the author of the limitation of freedoms. As a principle, any limitation of fundamental rights must therefore be *«prescribed by law»*, *"provided for by law"* or *«in accordance with law»*, these expressions having the same implications[582]. Such expressions essentially mean that any interference *"must have some basis in domestic law"*[583]. In addition, these expressions imply that the way the law is written must meet a certain number of requirements, which will enable the people concerned to exercise their rights.

The notion of legal basis

The term *«law»* is understood by the ECtHR *"in its substantive sense, not its formal one"*. Consequently, it not only refers to legislative texts, but also includes *"non-written law"*, *"enactments of lower rank than statutes"*, and case law. *"In a sphere covered by the written law, the «*law*»" is therefore "*the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments"*[584].

Such *"law"* must be adopted in compliance with domestic law and the rule of law, in order to offer *"protection in domestic law"*, including *«against arbitrary interferences by public authorities»*[585]. This implies that law is taken in compliance with democratic rules. Consequently, at least in serious matters, this implies that law is discussed and adopted by a parliament with effective decision-making power[586] in countries where the Constitution does grant legislative authority to this institution. Any circumvention of this rule should be temporary and duly justified.

The requirements related to the content of the law

The ECtHR developed three main requirements which all contribute to a fourth - the requirement of foreseeability: the law that organises the limitation must be sufficiently clear and precise, accessible, and stable[587].

Law must firstly be clear and precise. It must notably be *"formulated with sufficient precision to enable [citizens] to regulate [their] conduct: [they] must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail»*[588].

Foreseeability is of particular importance in the context of interferences by public authorities[589]. Indeed, in such cases, it *"cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly"*[590], but the *"risks of arbitrariness are evident"*[591]. As a result, in order *"to be compatible with the rule of law"*[592], the national law must be sufficiently clear and precise[593] *"in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort"* to such measures, so that they can adapt their conduct accordingly[594]. Clarity must be ensured in relation to all the guarantees and safeguards that are implemented in order to frame the power, in particular *"the scope of any discretion conferred on the competent authorities and the manner of its exercise"*[595].

Domestic law must also *"be adequately accessible"*, which means that *"the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case"*[596]. This implies firstly that the legal basis is easily accessible to concerned citizens[597], and secondly that the provisions authorising the limitation of freedom are intelligible, *"in the light of the legal corpus which they are intended to be part of"*[598]. Therefore, the whole of this corpus must be consistent[599], in order to fully meet the requirement of predictability[600]. In other words, the *"physical"*[601] access to the legal basis must be accompanied by an *"intellectual"*[602] access to this legal basis.

Finally, the law must be stable[603], in order to be *"reasonably"*[604] foreseeable. This principle is also linked to the requirement for legal certainty[605]. In addition, the principle of stability favours the general public's confidence in the legal system, and such confidence is *"one of the essential components of a state based on the rule of law"*[606].

In particular, the principle of stability implies that there are no unpredictable variations[607] and, potentially, no too frequent variations[608] of the law.

B. OTHER GUARANTEES (CONDITIONS AND SAFEGUARDS)

Any interference must be framed by *"adequate and effective guarantees against abuse"*[609], also referred to as *"conditions"* and/or *"safeguards"*[610]. Guarantees must be clarified in the legal basis that establishes the interference[611]. This principle is applicable to the activities of the judicial authority[612] and of intelligence services[613] in relation to any collection or storage of private information[614], in particular within the context of *"the development of surveillance methods resulting in masses of data collected"*[615].

Mandatory legal specifications

In the context of secret surveillance, and more precisely in the context of bulk interception of electronic communications, the ECtHR established a series of criteria to assess whether appropriate safeguards frame "the scope [...] and the manner of [...] exercise"616 of public authority's powers. Consequently, the ECtHR verifies the sufficient specification of:

(1) The grounds on which the measure may be authorised;

(2) The circumstances in which the measure can take place;

(3) The procedure to be followed for granting authorisation;

(4) The procedures to be followed for selecting, examining, and using intercept material;

(5) The precautions to be taken when communicating the material to other parties;

(6) The limits on the duration of interception, the storage of intercept material, and the circumstances in which such material must be erased and destroyed;

(7) The procedures and modalities for supervision, by an independent authority, of compliance with the above safeguards, and the actual powers of this authority to address non-compliance; and

(8) The procedures for independent ex post facto review of such compliance, and the powers vested in the competent body in addressing instances of non-compliance.[617]

The aim of these requirements is *"to give the individual adequate protection against arbitrary interference having regard to the legitimate aim of the measure in question"*[618], and to exclude any *"obscurity and uncertainty as to the state of the law"*[619].

These rules are undoubtedly applicable to the bulk collection of biometric identifiers. Indeed, such identifiers relate to the human body. They are very intimate, they are irrevocable, and they are therefore, at least, of the same sensitivity, if not higher, as metadata of communications. These rules are undoubtedly also applicable to biometric surveillance in public spaces, as a minimum, because such kind of surveillance is likely to disclose *"information on a person's conduct, opinions or feelings"*[620].

The ECtHR also clarified that *"a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it"*[621]. Rules established in the ECHR aim to preserve democracy[622] and the contracting states wishing to preserve this political model *"may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate"*[623].

Supervision

The above-mentioned list of criteria, which enables the assessment of whether appropriate safeguards frame the powers granted to public authorities, requires that control measures include the authorisation and/or the supervision of an independent authority[624], which will ensure that the legal conditions for the interference are respected.

The ECtHR clarified that *"review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated"*.

In relation to the two first stages, supervision must be particularly effective if surveillance is performed without the individuals' knowledge. Indeed, in such case, supervision replaces the possibility for the individual to seek remedy.[625] In addition, secret surveillance is *"a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole"*, that *"it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure"*.

[626] A supervision of another nature is only permitted if the authority in charge of it provides the same guarantee of independence and expertise[627].

In relation to the third stage, when surveillance measures have been terminated, effective *"safeguards against the abuse of surveillance powers"* may consist in a *"subsequent notification of surveillance measures"* to the individual concerned, enabling the latter to resort to the courts and thus retrospectively challenge the legality of these measures.[628] In addition, the establishment of a supervision at this sole third stage is not permitted in all matters[629], because confidentiality cannot be restored once destroyed[630].

Other safeguards

Control measures also include rights of access and verification granted to concerned individuals[631], the clarification of the procedure to be followed to exercise these rights[632], including a right of appeal when the right of access is denied[633], and - where possible - technical measures ensuring data deletion after a certain period of time[634].

In addition, means must be provided to ensure the effectiveness of guarantees and safeguards. These means may include judicial organisation and allocation of resources, where the latter are necessary to ensure the practical possibility and the efficiency of judicial controls.

4.1.3.5 Further restrictions to the possibility to limit a fundamental right: particularly protected rights, prohibition to suppress a right, and right to dignity

The general rule exposed in the previous subsections of the current study, which sets the conditions for limiting conditional fundamental rights, is further restricted in relation to some important rights, such

as the right to a fair trial and the right to physical liberty and security. Indeed, to limit these rights, stricter requirements need to be respected.[635]

These stricter requirements are generally mentioned in the ECHR. However, where it is not the case, the ECtHR establishes an adapted threshold, in order to ensure necessity and proportionality in the circumstance of the limitation of the particular right at stake. This takes place, for example, in relation to the right to not be subjected to degrading treatment[636] and in relation to the right to freedom of expression[637].

Moreover, beyond the particularities affecting one fundamental right or another, the ECtHR also verifies whether the *"overall effect»* of a given interference does not lead to *«actually extinguish»*[638] a fundamental right. For example, it *"was found to be unacceptable"* to prevent a person from making statements in a situation where such a measure effectively prevented this individual from *"making his contribution to the public debate"*.[639] This was affecting *«the very substance of the applicant's views"*.[640] In the same line, the CJEU verifies whether a given interference may *«adversely affect the essence of the fundamental right»*[641].

Through such decisions, the ECtHR affirms that there is, in relation to the fundamental right at stake, an *"essence/substance/core"* which *"should be respected under any circumstances [and which] constitutes the "*limit to the limits*".*[642] *Such a "*core" of fundamental rights is in other decisions protected based on the requirements of human dignity and self-determination which, likewise, cannot suffer any limitations[643].

4.2 EUROPEAN UNION

DATA PROTECTION REGULATION

Personal data protection, established in the EU Charter for fundamental rights, is further clarified in the European Union General Data Protection Regulation (GDPR)[644], which applies to all kinds of personal data processing operations, at the exclusion of strictly personal activities and of judicial processing activities[645]. Court and police data processing activities are regulated by the so-called *"Police-Justice"* Directive n° 2016/680, which applies more precisely to personal data processing *"by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security"*[646]. The GDPR and the Police-Justice Directive do not apply, in addition, to activities that fall outside the scope of Union law, which is the case of *"activities concerning national security, activities of agencies or units dealing with national security issues"*[647].

The protection awarded to personal data, including photographs, sounds[648], biometric data[649], and video surveillance[650], follows the same approach as the one offered by the ECHR[651], since the GDPR and the Police-Justice Directive are supposed to constitute specific applications of it, based on the states' positive obligation to ensure effective protection of fundamental rights, even in the relations of individuals between themselves[652]. As a consequence, any personal data processing must have a specified, explicit, and legitimate purpose[653], be efficient to meet this purpose[654], and be minimised to reach this purpose[655]. New necessity and proportionality tests are mandatory, together with an analysis of risks to rights and freedoms, where data processing is likely to have undue impacts on peoples' rights, even though the data processing operations comply with the GDPR or the Directive[656].

Moreover, biometric data benefit from a greater protection since they are considered to be *"sensitive data"*[657]. This limits the situations in which they may be processed, and it imposes the systematic performance of new necessity and proportionality analysis, together with a risk analysis, insofar they are processed at a large scale or in such a way as might result in a high risk to the rights and freedoms of natural persons[658]. In relation to guarantees and safeguards, and beyond the obligation to demonstrate that all previous obligations are satisfied, lies an important list of obligations relating to documentation, contractualisation, and limitation of some possibilities of processing, transparency and accountability.

In parallel, the European Union issued Directive 2002/58 on the processing of personal data and the protection of privacy in the electronic communications sector[659] (modified in 2009[660]). This Directive, called *"e-privacy"*, is currently under revision[661]. The CJEU confirmed that it is notably *"applicable to national legislation requiring providers of electronic communications services to carry out personal data processing operations, such as its transmission to public authorities or its retention, for the purposes of safeguarding national security and combating crime"*[662].

INSTRUMENTS ORGANISING DATA COLLECTION BY STATES

In addition to the legal instruments organising the protection of personal data, the European Union issued a series of successive legal instruments that aim to authorise states to collect or to access certain categories of citizens' and residents' personal data, for several purposes such as migration control and combatting crime.

We can highlight, in particular, the data retention directive 2006/24[663], adopted in 2006 and found disproportionate and contrary to the EUCFR by the CJEU in 2014[664] and in 2020[665]. In its latter decision, the CJEU ruled that Directive 2002/58 *"precludes legislative measures requiring providers of electronic communications services to carry out the general and indiscriminate retention of traffic data and location data as a preventive measure. Those obligations to forward and to retain such data in a general and indiscriminate way constitute particularly serious interferences with the fundamental rights guaranteed by the Charter, where there is no link between the conduct of the persons whose data are affected and the objective pursued by the legislation at issue"*[666]. Similarly, the European Court interprets article 23(1) of the GDPR, *"read in the light of the Charter, as precluding national legislation requiring providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, inter alia, personal data relating to those services"*[667]. The CJEU accepts that Directive 2002/58 and the EUCFR enable *"recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic data and location data"*. However, the Court considers that such recourse can only take place *"in situations where the Member state concerned is facing a serious threat to national security that proves to be genuine and present or foreseeable"*. In addition, the CJEU considers that such an order must be issued *"for a period that is limited in time to what is strictly necessary, must be subject to effective review either by a court or by an independent administrative body whose decision is binding, in order to verify that one of those situations exists and that the conditions and safeguards laid down are observed"*[668].

INSTRUMENTS ORGANISING BIOMETRIC DATA COLLECTION BY STATES

The European Union also issued a series of successive legal instruments aiming to impose on states the collection of biometric identifiers for the purpose of migration control. This purpose has been further extended to several other purposes such as the prevention of threats to the internal security of member states, the prevention, detection and investigation of terrorist offences and other serious criminal offences, and – in relation to certain legal instruments only - to simple exchanges for police purposes.[669] Globally, these instruments do not appear to provide for sufficient effective guarantees for preserving fundamental rights[670], despite the fact that biometric identifiers are widely considered as being sensitive, by the European Commission itself[671].

For example, Regulation 2019/1157 of 20 June 2019 on strengthening the security of identity cards[672] mainly refers, in relation to safeguards, to security issues[673], to liability under the GDPR[674], and to the role of Data Protection Authorities[675]. It prohibits the member states from storing formore than 90 days,

the biometric identifiers that are collected for the purpose of issuing identity cards, but it authorises other processing that would be decided at national levels. In this regard, it merely specifies that the Regulation *"does not provide a legal basis for"* such processing[676], and that such other processing must be *"necessary and proportionate to the aim to be achieved"*[677], *"in accordance with Union and national law"*[678]. However, it does not detail the concrete guarantees to be implemented, whereas it creates the possibility of function creep[679]. In addition, the Regulation – and therefore these statements – is not supposed to apply to services in charge of national security, which fall outside the scope of Union law.

Despite these issues, and the fact that the European Data Protection Supervisor itself asked to *"reassess the necessity and the proportionality"* of the proposal for this regulation in relation to the processing of biometric data[680], the regulation has been adopted and it seems that the EC's intention is to continue its initiative to build biometric databases. Indeed, non-governmental organisations signed in September 2021 an open letter to the members of the European Parliament who work on *"new rules for the Eurodac database"*[681] ,in order to call for a *"halt to negotiations so that the impact on human rights can be meaningfully taken into account"*[682]. They highlight that the envisioned new legislation framing Eurodac, which stored *"in* 2020 *almost* 650*,*[000] *sets of fingerprints"*[683] of asylum seekers and irregular migrants[684], will lead to processing *"more data categories for a wider set of purposes"*[685]. According to the letter, plans are to collect facial images as well as new information such as identity information, in relation to more categories of people including children, with a possibility to use coercive means in order to gather such information, and to organise more extensive rights of access for law-enforcement, assisted by technologies such as statistics and flagging that might lead to arbitrary stigmatisation. The signatories of the letter call for *"delay to the legislative process to give due time for significant consideration of the fundamental rights implications of the proposed EURODAC reform"*. They notably highlight that, for now, *"the European Commission has failed to demonstrate that the capture of facial images meets the necessity and proportionality test"*[686].

Finally, on 21 April 2021, the European Commission issued a proposition aimed at laying down harmonised rules on artificial intelligence[687]. This proposed *"Artificial Intelligence Act"* frames the *"placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union"*. At the same time, it prohibits certain artificial intelligence practices, and it sets up *"specific requirements for high-risk AI systems and obligations for operators of such systems"*. It also organises *"harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content"*.[688]

The choice has therefore been *"to follow a risk-based approach [which] differentiates between uses of AI that create (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk. Depending on the risk classification, an AI application may need to be in conformity with a range of mandatory requirements"*[689]. In particular, the proposed regulation considers that *"'real-time' and 'post' remote biometric identification systems should be classified as high-risk"* and that, for this reason, *"both types of remote biometric identification systems should be subject to specific requirements on logging capabilities and human oversight"*[690]. It further prohibits as a principle the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement[691]. However, such prohibition does not apply to *"post"* identification[692], neither to 'real-time' remote biometric identification that would be operated by the private sector or by public authorities for national security purposes[693]. In addition, article 5 of the proposed regulation authorises member states to bypass this prohibition and to authorise by law the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within certain limits.

The first of these limits is to specify the precise objectives of the authorisation, which must imperatively lie in the list of objectives provided in the regulation (these objectives are (1) the targeted search for specific potential victims of crime including missing children, (2) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a

terrorist attack, and (3) the detection, localisation, identification or prosecution of a perpetrator or suspect of a serious criminal offence)[694].

A second limit is to use 'real-time' remote biometric identification systems taking into account certain aspects listed in article 5.2 of the regulation, such as the seriousness, the probability and the scale of the harm caused in the absence of the use of the system.

A third limit is the obligation to set-up necessary and proportionate safeguards and conditions in relation to the use of biometric identification technology, in particular *"as regards the temporal, geographic and personal limitations"*. In any case, operations must be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority, issued upon a reasoned request, unless a duly justified situation of urgency imposes the need to initiate operations beforehand.

This proposed Artificial Intelligence Regulation does not appear to frame the use of biometric recognition technology with sufficient safeguards, while creating the conditions for its implementation. This has in particular been highlighted by the European Data Protection x - 82 - X November, 2021

Board (EDPB) and the European Data Protection Supervisor (EDPS) in a joint opinion dated June 2021[695]. It will be the subject of further analysis in subsection 5 of the current study.

4.3 NATIONAL LEGISLATIONS

The EU member states are all parties to the ECHR and must respect the EUCFR. In addition, rights established in the Convention and in the Charter are globally enforced by national Supreme Courts, based on the national Constitution or on an interpretation of the latter[696]. They are also subject to the GDPR and to the Police-Justice Directive.

All member states have also implemented the EU legislation relating to the use of biometric identifiers in identity cards and migration documents[697]. In addition, whereas Regulation 2019/1157 of 20 June 2019 on strengthening the security of identity cards does prohibit states from storing beyond 90 days the biometric identifiers that were collected for the purpose of the regulation[698], it appears that several states decided to anticipate or to seize this opportunity to create biometric national databases[699], sometimes based on a legal instrument that was not submitted to the national Parliament[700]. In certain member states, CCTV surveillance in public places is regulated by a specific law[701] while it is only regulated by the GDPR in others[702].

At the same time, member states implemented the data retention directive, which is still in force in some states despite the CJUE declaring it contrary to the EUCFR. Indeed, not all countries[703] have modified their law in order to take into account the CJEU prohibition to organise a *"general and indiscriminate retention of traffic data and location data as a preventive measure"*.[704] In addition, members states generally grant law enforcement powers to access public and private databases that are not under their control, within the framework of criminal investigations. Other public authorities benefit from the same right of access, for the purpose of national security and of the prevention of terrorism[705].

305. France, United Kingdom, Belgium, Netherlands, Luxembourg, Denmark, Italy, Norway, Sweden and Ireland. See 'The origins of the Council of Europe', CVCE.EU by UNI.LU, last update 7 July 2016, p. 2-3, http://www.cvce.eu/obj/the_origins_of_the_council_of_europe-en-aa7eeb5f-f6c0-4ac5-a1ec-4cc9beb0d739.html. See also 'Towards the European Assembly and the Council of Europe', CVCE.EU by UNI.LU, last update 8 July 2016, http://www.cvce.eu/obj/towards_the_european_assembly_and_the_council_of_europe-en-f27e860d-5d53-4ccb-9848-48a1febc7c9b.html.

306. The origins of the Council of Europe, CVCE.EU by UNI.LU, already mentioned, p 2.

307. The origins of the Council of Europe, CVCE.EU by UNI.LU, already mentioned, p 2.

308. 'The establishment of the European Convention for the Protection of Human Rights', CVCE.EU by UNI.LU, https://www.cvce.eu/en/obj/the_establishment_of_the_european_convention_for_the_protection_of_human_rights-en-ea6b1c3a-dd6c-4cb8-a55d-ea75a655aab5.html.

309. Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 5 November 2050, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005, also available from https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=.

310. Convention for the Protection of Human Rights and Fundamental Freedoms, Protocols, https://www.coe.int/en/web/portal/home?p_p_id=15&p_p_lifecycle=0&p_p_state=pop_up&p_p_mode=view&_15_groupId=99928066&_15_struts_action=/journal/preview_article_content&_15_articleId=99928550&_15_version=1.6.

311. Council of Europe, 'Who we are', http://www.coe.int/en/web/about-us/who-we-are.

312. Indeed, they have all accessed to or ratified the ECHR. See Chart of signatures and ratifications of Treaty 005, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=005.

313. Convention for the Protection of Human Rights and Fundamental Freedoms, Protocols, already mentioned.

314. The ECHR preliminary draft convention was drawn up by former French Minister Pierre-Henri Teitgen, who was Chairman of the European Movement's Legal Committee, and accepted as a basis for further work. See 'The establishment of the European Convention for the Protection of Human Rights', CVCE.EU by UNI.LU, https://www.cvce.eu/en/obj/the_establishment_of_the_european_convention_for_the_protection_of_human_rights-en-ea6b1c3a-dd6c-4cb8-a55d-ea75a655aab5.html.

315. 'The establishment of the European Convention for the Protection of Human Rights', CVCE.EU by UNI.LU, already mentioned; Jacques Robert and Jean Duffar, Droits de l'homme et libertés fondamentales, Montchrestien, Lextenso éditions, 8° ed., 2009, p. 83.

316. François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 6; François Sureau, in La Grande table Idées d'Olivia Gesbert, émission du 30 septembre 2019, France Culture, https://www.youtube.com/watch?v=VUgQAr4zPV4.

317. Jacques Robert and Jean Duffar, Droits de l'homme et libertés fondamentales, Montchrestien, Lextenso éditions, 8° ed., 2009, p. 3.

318. 'The establishment of the European Convention for the Protection of Human Rights', CVCE.EU by UNI.LU, https://www.cvce.eu/en/obj/the_establishment_of_the_european_convention_for_the_protection_of_human_rights-en-ea6b1c3a-dd6c-4cb8-a55d-ea75a655aab5.html. See also the preamble of the ECHR.

319. 'The establishment of the European Convention for the Protection of Human Rights', already mentioned.

320. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

321. Article 51 of the Charter.

322. EU Charter of Fundamental Rights, article 52, 3. In addition, "nothing in the Charter shall be interpreted as restricting or adversely affecting fundamental freedoms as recognised" by the Convention: see article 53 of the Charter and Sébastien Van Drooghenbroeck and Cecilia Rizcallah, 'The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?', 30 May 2019, German Law Journal (2019), 20, Cambridge University Press, pp. 904–923, p. 905, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/594CA9F2A83DF4B52A1FB6B638339FB4/S2071832219000683a.pdf/echr_and_the_essence_of_fundamental_rights_searching_for_sugar_in_hot_milk.pdf.

323. Larry Diamond, 'Defining and Developing Democracy', in Robert Alan Dahl, Ian Shapiro and José Antônio Cheibud, The democracy sourcebook, MIT Press, August 2003, p. 29. See also Jacques Robert and Jean Duffar, 'Etat libéral et démocratie' in Droits de l'homme et libertés fondamentales, already mentioned, p. 16; Estelle De Marco, 'The role of democracy', in C. Callanan et al., Internet blocking: balancing cybercrime responses in democratic societies, 2009, p. 134 s., https://www.inthemis.fr/ressources/Internet_blocking_and_Democracy.pdf.

324. Robert Badinter, 'Preface', in Beccaria, Des délits et des peines, Flammarion, 1991, p.38 s., esp. p. 46.

325. Beccaria, Des délits et des peines, Flammarion, 1991, esp. p. 60 and p. 63.

326. Alexis de Tocqueville, Democracy in America, translated by Henry Reeve, Saunders and Otley, London, 1835. See the introduction of the current study.

327. François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 42.

328. François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 46. According to the author, it is not legitimate to prohibit freedom "in the name of this mysterious balance

between security and freedom which is foreign to the principles of our legal system" (translated from French).

329. Daniel J. Solove, Nothing to Hide, The False Tradeoff between Privacy and Security, Yale University Press, 2011, p.3.

330. François Sureau, Intervention lors de la conférence «Nouveaux Dissidents - Nouveaux Résistants» organisée par Najat Vallaud-Belkacem (Raison de Plus) et Olivier Christin (Centre Européen d'études républicaines - Université PSL) le 20 janvier 2020 au CNAM à Paris, https://www.youtube.com/watch?v=P_DQQ4m6luk; (translated from French): «the introduction, in the debate, of the security-freedom couple [...] the idea that security would be the first of freedoms, this nonsense consisting in saying that, actually, there was no more free political system than the one of Stalin's Moscow, where security and freedom were ensured in absolute terms, [...] is obviously an absurdity, both in practical and in conceptual terms»; see also François Sureau, 'La sécurité n'est «la première des libertés» que pour ceux qui ont perdu de vue ce que le mot de liberté signifie', 1 November 2017, https://www.la-croix.com/Debats/Chroniques/securite-nest-premiere-libertes-ceux-perdu-vue-mot-liberte-signifie-2017-11-01-1200888721.

331. See subsection 4.1.3 of the current study.

332. See for example Olivier Aïm, Les théories de la Surveillance – Du panoptique aux Surveillance Studies, ed. Armand Colin, 2020, p. 105; François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p.40-49.

333. Jacques Robert and Jean Duffar, Droits de l'homme et libertés fondamentales, Montchrestien, Lextenso éditions, 8° ed., 2009, p. 3.

334. The expression used depends on the legal tradition. In relation to the difference between the continental European tradition and the Anglo-American legal tradition, see Mats G. Hansson, The Private Sphere: An Emotional Territory and Its Agent, Springer, 15 November 2007, p. 113.

335. Samuel D. Warren and Louis D. Brandeis, 'The right to privacy', in Harvard Law Review, vol. IV, 15 Dec. 1890, n°5. See also Stéphane-Dimitri Chupin, La protection de la vie personnelle délimitée par les frontières des sphères privées et publiques, thesis, Université Paris I, 2002, p. 32.

336. Statement from Prof. Stig Strömholm, reported by Advocate General Cabannes in its conclusions under a decision of the Court of Appeal of Paris, 15 May 1970, D. 1970, jurisp. p. 466, p. 468. Prof. Stig Strömholm's conception of privacy is also mentioned by Alexandre Maitrot de la Motte, 'Le droit au respect de la vie privée', in La protection de la vie privée dans la société d'information, Pierre Tabatoni (dir.), Tome 3, 4 et 5, Cahier des sciences morales et politique, PUF, Jan. 2002, p. 271, and by Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 329.

337. Estelle De Marco, 'The definition of private life', March 2019, EU INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, https://www.inthemis.fr/ressources/definition-of-private-life.html; See also the works of Mats G. Hansson, The Private Sphere: An Emotional Territory and Its Agent, Springer, 2007; Florence Deboissy, 'La divulgation d'une information patrimoniale', D. 2000, chron. p. 26; Emmanuel Dreyer, 'Le respect de la vie privée, objet d'un droit fondamental', Com. com. élec., n° 5, May 2005, I, 18; Ruth E. Gavinson, 'Privacy and the limits of law', The Yale Law Journal, Vol. 89, n° 3 (Jan. 1980), p. 421-471, http://www.jstor.org/stable/795891 or http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2060957; Ahti Saarenpää, Perspectives on privacy, Prensas Universitarias de Zaragoza, 2008, LEFIS Series p. 19-63, particularly p. 21.

338. In relation to this approach and the other existing ones, see Estelle De Marco, 'The definition of private life', already mentioned; Estelle De Marco, Comparative study between Directive 95/46/EC & the GDPR including their relations to fundamental rights, March 2018, Deliverable D2.10, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, subsection n° 2.2.1, https://www.inthemis.fr/ressources/INFORM_D2.10_Comparative_analysis_GDPR_Dir9546EC.pdf.

339. For example, legally protected privacy information is not the same towards a spouse and an employer. However, the information that is not protected against a spouse may remain protected against an employer.

340. Based on article 8 of the ECHR.

341. Based on article 7 of the EUCFR.

342. ECHR, 5° Section, 10 January 2019, Khadija Ismayilova v. Azerbaijan, appl. n° 65286/13 and 57270/14, § 139, http://hudoc.echr.coe.int/eng?i=001-188993.

343. ECHR, 5° Section, Khadija Ismayilova v. Azerbaijan, already mentioned, § 140.

344. ECtHR, 3rd Sect., 25 September 2001, P.G. and J.H. v. the United Kingdom, appl. n°. 44787/98, §56, http://hudoc.echr.coe.int/eng?i=001-59665. See also ECtHR, 4th Sect., 29 April 2002, Pretty v. The United Kingdom, appl. n° 2346/02, §61, http://hudoc.echr.coe.int/eng?i=001-60448.

345. ECtHR, Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, Council of Europe/European Court of Human Rights, 31 December 2020, p. 21, https://www.echr.coe.int/documents/guide_art_8_eng.pdf; ECtHR, 4th Sect., 29 April 2002, Pretty v. The United Kingdom, already mentioned, § 61 and 67.

346. See for ECtHR, ch., 16 December 1992, Niemietz v. Germany, appl. n°13710/88, §32, http://hudoc.echr.coe.int/eng?i=001-57887; see also ECtHR, gr. ch., 16 February 2000, Amann v. Switzerland, appl. n° 27798/95, §65, http://hudoc.echr.coe.int/eng?i=001-58497.

347. ECtHR, Niemietz v. Germany, already mentioned, §29.

348. ECtHR, gr. ch., 5 September 2017, Bărbulescu v. Romania, 61496/08, § 71, http://hudoc.echr.coe.int/eng?i=001-177082.

349. ECHR, ch., 24 February 1998, Botta v. Italy, appl. n° 65286/13 and 57270/14, § 32, http://hudoc.echr.coe.int/eng?i=001-58140.

350. ECtHR, 1st Sect., 7 February 2002, Mikulić v. Croatia, application n° 53176/99, § 53, http://hudoc.echr.coe.int/eng?i=001-60035.

351. ECtHR, gr.ch., 16 December 2010, A, B, and C v. Ireland, application n° 25579/05, http://hudoc.echr.coe.int/eng?i=001-102332; ECtHR, ch., 26 March 1985, X and Y v. the Netherlands, appl. n°8978/80, §

22, http://hudoc.echr.coe.int/eng?i=001-57603.

352. ECHR, 5° Section, 10 January 2019, Khadija Ismayilova v. Azerbaijan, appl. n° 65286/13 and 57270/14, § 139, http://hudoc.echr.coe.int/eng?i=001-188993.

353. ECtHR, 24 February 1998, Botta v. Italy, already mentioned, § 32.

354. ECtHR, gr. ch., 16 February 2000, Amann v. Switzerland, appl. n° 27798/95, §65, http://hudoc.echr.coe.int/eng?i=001-58497.

355. ECtHR, 4th Sect., 29 April 2002, Pretty v. The United Kingdom, appl. n° 2346/02, §61, 65-66, http://hudoc.echr.coe.int/eng?i=001-60448; ECtHR, 1st Section, Gladysheva v. Russia, 6 December 2011, appl. n°7097/10, § 93, http://hudoc.echr.coe.int/eng?i=001-107713.

356. ECHR, gr. ch., 7 February 2012, Von Hannover v. Germany (no. 2), appl. n° 40660/08 and 60641/08, § 95, http://hudoc.echr.coe.int/eng?i=001-109029.

357. ECtHR, Niemietz v. Germany, already mentioned, §28 and 29.

358. ECtHR, Niemietz v. Germany, already mentioned, §28 and 29; See Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p.43-44. Before the ECtHR ruled on this subject, the Court of Justice of the European Union stated that the need for a protection of legal persons' private sphere of activities «must be recognised as a general principle of Community law»: judgment of 21 September 1989, Hoechst v. Commission, joined cases 46/87 and 227/88, European Court Reports 1989, pp. 2859-2924.

359. See for instance Commission, plen., 27 February 1995, B.C. v. Switzerland, Application n°21353/93, http://hudoc.echr.coe.int/eng?i=001-2039; ECtHR, ch., 25 March 1983, Silver and others v. the United Kingdom, appl. n°5947/72, § 84, http://hudoc.echr.coe.int/eng?i=001-57577.

360. See for instance ECtHR, Silver and others v. the United Kingdom, already mentioned, § 84.

361. ECtHR, 2nd Sect., 22 October 2002, Taylor-Sabori v. the United Kingdom, appl. n°47114/99, §18, http://hudoc.echr.coe.int/eng?i=001-60696.

362. ECtHR, Niemietz v. Germany, already mentioned, §32.

363. ECtHR, ch., 25 March 1998, Kopp v. Switzerland, appl. n°23224/94, §50, http://hudoc.echr.coe.int/eng?i=001-58144; ECtHR, ch., 25 June 1997, Halford v. the United Kingdom, appl. n°20605/92, §§ 44-46, http://hudoc.echr.coe.int/eng?i=001-58039.

364. See for instance ECtHR, plen., 2 August 1984, Malone v. The United Kingdom, appl. n°8691/79, §41, http://hudoc.echr.coe.int/eng?i=001-57533; ECtHR, ch., 16 December 1992, Niemietz v. Germany, appl. n°13710/88, §32, http://hudoc.echr.coe.int/eng?i=001-57887.

365. ECtHR, 3rd Sect., 25 September 2001, P.G. and J.H. v. the United Kingdom, appl. n°. 44787/98, http://hudoc.echr.coe.int/eng?i=001-59665.

366. See ECtHR, 4th Sect., 3 April 2007, Copland v. the United Kingdom, appl. n° 62617/00, § 41, http://hudoc.echr.coe.int/eng?i=001-79996; In relation to internet instant messaging (Yahoo) see ECtHR, gr. ch., 5 September 2017, Bărbulescu v. Romania, 61496/08, § 18, 74, http://hudoc.echr.coe.int/eng?i=001-177082.

367. ECtHR, gr. ch., 16 February 2000, ECtHR, gr. ch., 16 February 2000, Amann v. Switzerland, appl. n° 27798/95, §65, http://hudoc.echr.coe.int/eng?i=001-58497.

368. ECtHR, 4° sect., 24 April 2018, Benedik v. Slovenia, appl. n° 62357/14, §107, http://hudoc.echr.coe.int/eng?i=001-182455.

369. ECtHR, Amann v. Switzerland, already mentioned, § 65.

370. ECtHR, 4° sect., 24 April 2018, Benedik v. Slovenia, appl. n° 62357/14, §107-108, http://hudoc.echr.coe.int/eng?i=001-182455.

371. ECtHR, Amann v. Switzerland, already mentioned, § 65.

372. ECtHR, ch., 26 March 1987, Leander v. Sweden, appl. n°9248/81, §48, http://hudoc.echr.coe.int/eng?i=001-57519; ECtHR, gr.ch., 4 May 2000, Rotaru v. Roumania, appl. n°28341/95, §45 s., http://hudoc.echr.coe.int/eng?i=001-58586.

373. ECtHR, gr.ch., 16 February 2000, Amann v. Switzerland, already mentioned, § 69; See also (in relation to phone calls), ECtHR, ch., 25 March 1998, Kopp v. Switzerland, appl. n° 13/1997/797/1000, §53, http://hudoc.echr.coe.int/eng?i=001-58144.

374. ECtHR, 5th Sect., 17 December 2009, Gardel v. France, appl. n° 16428/05, § 58, http://hudoc.echr.coe.int/eng?i=001-96457; ECtHR, gr. ch., 16 February 2000, Amann v. Switzerland, appl. 27798/95, § 70, http://hudoc.echr.coe.int/eng?i=001-58497; CJEU, 20 May 2003, Österreichischer Rundfunk and Others, joined cases C-465/00, C-138/01 and C-139/01, § 75, https://curia.europa.eu/juris/liste.jsf?num=C-465/00&language=en; CJEU, 8 April 2014, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, § 33, http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12.

375. ECtHR, Rotaru v. Roumania, already mentioned, §43-44; ECtHR, Catt v. the United Kingdom, already mentioned, § 93.

376. ECtHR, 3rd Sect., 15 April 2014, Radu v. The Republic of Moldova, appl. n° 50073/07, §27, http://hudoc.echr.coe.int/eng?i=001-142398; ECtHR, 4th Sect., 27 February 2018, Mockutė v. Lithuania, appl. n° 66490/09 2018, § 93-95, http://hudoc.echr.coe.int/eng?i=001-181202.

377. ECtHR, gr. ch., 27 June 2017, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, appl. n° 931/13, § 134, http://hudoc.echr.coe.int/eng?i=001-175121. ;

378. ECtHR, 4th Sect., 28 January 2003, Peck v. The United Kingdom, appl. n° 44647/98, § 59, http://hudoc.echr.coe.int/eng?i=001-60898; ECtHR, Rotaru v. Roumania, already mentioned, §43-44; ECtHR, Catt v. the United Kingdom, already mentioned, § 93.

379. ECtHR, gr. ch., 27 June 2017, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, already mentioned, § 137.

380. ECtHR, 3rd Sect., 25 September 2001, P.G. and J.H. v. the United Kingdom, appl. n° 44787/98, § 57, http://hudoc.echr.coe.int/eng?i=001-59665; ECtHR, Rotaru v. Roumania, already mentioned, §44.

381. ECtHR, 3rd Sect., 25 September 2001, P.G. and

J.H. v. the United Kingdom, already mentioned, § 58.

382. *ECtHR, 4e sect., 12 janvier 2016, Szabó and Vissy v. Hongrie, appl. no 37138/14, §68, http://hudoc.echr.coe.int/eng?i=001-160020.*

383. *ECtHR, 1st Sect., 24 January 2019, Catt v. the United Kingdom, n° 43514/15, § 93, http://hudoc.echr.coe.int/eng?i=001-189424.*

384. *ECtHR, 5th Sect., 2 September 2010, Uzun v. Germany, appl. n° 35623/05, § 51, http://hudoc.echr.coe.int/eng?i=001-100293.*

385. *ECtHR, 5th Sect., 2 September 2010, Uzun v. Germany, already mentioned, §52.*

386. *ECtHR, 5th Sect., 18 April 2013, M.K. v. France, appl. n° 19522/09, §29, http://hudoc.echr.coe.int/eng?i=001-119075.*

387. *ECtHR, gr. ch., 4 December 2008, S. and Marper v. The United Kingdom, appl. n° 30562/04 and 30566/04, § 84-85, http://hudoc.echr.coe.int/eng?i=001-90051.*

388. *ECtHR, 3rd Sect., 25 September 2001, P.G. and J.H. v. the United Kingdom, appl. n° 44787/98, § 60, http://hudoc.echr.coe.int/eng?i=001-59665.*

389. *Based on article 10 of the ECHR.*

390. *Based on article 11 of the EUCFR.*

391. *Article 10§1 of the ECHR.*

392. *ECtHR, Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, Council of Europe/European Court of Human Rights, December 2011, p. 4, http://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf.*

393. *Article 10 of the ECHR.*

394. *The ECtHR evokes the right for the public to receive "information and ideas on matter of public interest": ECtHR, plen., 26 November 1991, Observer and Guardian v. The United Kingdom, appl. n° 13585/88, § 59, http://hudoc.echr.coe.int/eng?i=001-57705.*

395. *ECtHR, plen., 26 November 1991, Observer and Guardian v. The United Kingdom, already mentioned, § 59.*

396. *ECtHR, plen., 26 November 1991, Observer and Guardian v. The United Kingdom, already mentioned, § 59.*

397. *European Convention on Human Rights, article 10§2.*

398. *Precautions to be taken by publishers are recalled in several instruments and court decisions. See for example the suggestions to media and journalists in the Council of Europe Committee of Ministers Declaration on freedom of expression and information in the media in the context of the fight against terrorism, 2 March 2005, https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Decl-02.03.2005&Sector=secCM&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75&direct=true; As another example, the Belgium Court of cassation considered that persons at the origin of a publication "are required to communicate to the public a correct, objective and as exact as possible information. They must refrain from making serious accusations without having verified them sufficiently" (Translated from French, Decision of 27 April 2007, N° C.06.0123.N, 1.H. R., 2.G. E. v. D. J., p. 3, https://juricaf.org/arret/BELGIQUE-COURDECASSATION-20070427-C060123N.*

399. *See for example European Commission for Democracy through Law (Venice Commission), Report on the relationship between freedom of expression and freedom of religion: the issue of regulation and prosecution of blasphemy, religious insult and incitement to religious hatred, 23 October 2008, Study n° 406/2006, CDL-AD(2008)026, https://www.venice.coe.int/WebForms/documents/default.aspx?pdffile=CDL-AD(2008)026-e, especially n° 44, 74, 85 et 86; Council of Europe, Bookmarks – A manual for combating hate speech online through human rights education, revised edition 2016, n° 5.3 p. 160, https://rm.coe.int/168065dac7; ECtHR, ch., Otto-Preminger-Institut v. Austria, 20 September 1994, appl. n°13470/87, § 47, http://hudoc.echr.coe.int/eng?i=001-62451; Estelle De Marco, Identification and analysis of the legal and ethical framework, Deliverable D2.2, version 2.2.4 of 12 July 2017, MANDOLA EU project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, subsection 4.3.3.1.2.3, p. 138, footnotes 808-814; Estelle De Marco, Definition of illegal hatred and implications, Delivrable D2.1b (final report), version 4 of 30 November 2016, MANDOLA EU project afore mentioned, subsection 6.2.3, p. 67.*

400. *ECtHR, ch., Otto-Preminger-Institut v. Austria, 20 September 1994, appl. n°13470/87, § 49, http://hudoc.echr.coe.int/eng?i=001-57897, which evokes «an obligation to avoid as far as possible expressions that are gratuitously offensive to others and thus an infringement of their rights, and which therefore do not contribute to any form of public debate capable of furthering progress in human affairs».*

401. *See for example Venice Commission, Report on the relationship between freedom of expression and freedom of religion: the issue of regulation and prosecution of blasphemy, religious insult and incitement to religious hatred, already mentioned, especially n° 74; ECtHR, ch., Otto-Preminger-Institut v. Austria, 20 September 1994, already mentioned, §49; Cormac Callanan et al., Best Practice Guide for responding to Online Hate Speech for internet industry, Deliverable D4.2, v1.0, March 2017, MANDOLA EU project afore-mentioned, subsection n° 5.2.2.*

402. *As well as some Constitutional Courts, see for example French Conseil Constitutionnel, Decision n°2015-512 QPC of 8 January 2016, § 5, https://www.conseil-constitutionnel.fr/decision/2016/20155120PC.htm.*

403. *Council of Europe, Bookmarks – A manual for combating hate speech online through human rights education, already mentioned, n° 5.3, p. 160.*

404. *ECtHR, plen., 7 December 1976, Handyside v. The United Kingdom, appl. n° 5493/72, § 49, http://hudoc.echr.coe.int/eng?i=001-57499; ECtHR, gr. ch., 22 October 2007, Lindon, Otchakovsky-Laurens and July v. France, appl. n°21279 and 36448/02, § 45, http://hudoc.echr.coe.int/fre?i=001-82846.*

405. *ECtHR, gr. ch., 22 October 2007, Lindon, Otchakovsky-Laurens and July v. France, already mentioned, § 51.*

406. *Council of Europe, Bookmarks – A manual for combating hate speech online through human rights education, already mentioned, n° 5.3 p. 161. In the same line see Albert Einstein, Mein Weltbild (The World as I see it), 'Wie ich die Welt sehe' (The World as I see*

it), Gemeinschaft und persönlichkeit (Community and personality), Ullstein Sachbuch, 1989.

407. ECtHR, plen., 7 December 1976, Handyside v. The United Kingdom, already mentioned, § 49; ECtHR, gr. ch., 22 October 2007, Lindon, Otchakovsky-Laurens and July v. France, already mentioned, § 45.

408. ECtHR, gr. ch., 22 October 2007, Lindon, Otchakovsky-Laurens and July v. France, already mentioned, § 45.

409. European Parliament Resolution of 21 May 2013 on the EU Charter: standard setting for media freedom across the EU (2011/2246(INI)), B, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0203.

410. ECtHR, 2nd Sect., 14 September 2010, Dink v. Turkey, appl. n° 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, §137, http://hudoc.echr.coe.int/eng?i=001-100384; ECtHR, Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, Council of Europe/European Court of Human Rights, December 2011, p. 5, http://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf.

411. ECtHR, 2nd Sect., 5 July 2005, Melnychuk v. Ukraine, appl. n°. 28743/03, http://hudoc.echr.coe.int/eng?i=002-3781; ECtHR, Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, already mentioned, p. 5; Recommendation of the Committee of Ministers of the Council of Europe on the right to reply in the new media environment, 15 December 2004, available in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Strasbourg, 2016, p. 119, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44.

412. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, available in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, already mentioned, p. 288, http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp; In the same document see Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, p. 150 quot. p. 152, see also p. 153; Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, 27 September 2006, p. 124; Appendix to Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, p 162, part III, especially p. 164 s.

413. European Parliament Resolution of 21 May 2013 on the EU Charter: standard setting for media freedom across the EU (2011/2246(INI)), n°30, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0203.

414. Council of Europe, Committee of Ministers, Declaration on the freedom of expression and information, 29 April 1982, n°6, available in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, Strasbourg, 2016, §6 p. 272, https://rm.coe.int/0900001680645b44. See also ECtHR, Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, already mentioned, p. 4.

415. Article 11§2: "the freedom and pluralism of the media shall be respected". According to the European Parliament, this requirement is based, in particular, "on Court of Justice case law regarding television [in particular CJEU, 25 July 1991, Stichting Collectieve Antennevoorziening Gouda and others v. Commissariaat voor de Media, Case C-288/89, esp. §23, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61989CJ0288], on the Protocol on the system of public broadcasting in the Member States annexed to the EC Treaty and now to the Constitution, and on Council Directive 89/552/EC (particularly its seventeenth recital": Explanations relating to the Charter of Fundamental Rights of the European Union, Art. 11, §2, http://www.europarl.europa.eu/charter/convent49_en.htm and http://www.europarl.europa.eu/charter/pdf/04473_en.pdf).

416. Based on article 11 of the ECHR.

417. Based on article 12 of the EUCFR.

418. OSCE, Handbook on Monitoring Freedom of Peaceful Assembly, second edition, 2020, p. 32, https://policehumanrightsresources.org/handbook-on-monitoring-freedom-of-peaceful-assembly-second-edition.

419. OSCE, Handbook on Monitoring Freedom of Peaceful Assembly, already mentioned, p. 32.

420. OSCE, Handbook on Monitoring Freedom of Peaceful Assembly, already mentioned, p. 32.

421. Council of Europe, Freedom of assembly and association, http://www.coe.int/en/web/echr-toolkit/la-liberte-de-reunion-et-dassociation.

422. OSCE, Handbook on Monitoring Freedom of Peaceful Assembly, second edition, 2020, p. 34.

423. OSCE, Handbook on Monitoring Freedom of Peaceful Assembly, second edition, 2020, p. 34.

424. Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member states on Internet freedom, n°3, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa; See also Appendix to the Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, 7 November 2007, I (Human Rights and democracy), http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008_CMrec0711_en.PDF; Declaration CM(2005)56 of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp.

425. Declaration CM(2005)56 of the Committee of Ministers on human rights and the rule of law in the Information Society, already mentioned, n°8 (Freedom of assembly).

426. Declaration CM(2005)56 of the Committee of

Ministers on human rights and the rule of law in the Information Society, already mentioned, n°8

427. *Article 9 of the ECHR and article 10 of the EUCFR.*

428. *ECtHR, Guide on Article 9 of the European Convention on Human Rights - Freedom of Thought, Conscience and Religion, Council of Europe/European Court of Human Rights, 2021, n° 25, https://www.echr.coe.int/Documents/Guide_Art_9_ENG.pdf. See also ECtHR, 5th Sect., 12 April 2007, Ivanova v. Bulgaria, appl. n 52435/99,§ 79, http://hudoc.echr.coe.int/eng?i=001-80075.*

429. *ECtHR, Guide on Article 9 of the European Convention on Human Rights, already mentioned, n° 25.*

430. *ECtHR, Guide on Article 9 of the European Convention on Human Rights, already mentioned, n° 27.*

431. *ECtHR, Guide on Article 9 of the European Convention on Human Rights, already mentioned, n° 28-29.*

432. *Enshrined in article 45 of the EUCFR and in the Protocol n°4 to the Convention for the Protection of Human Rights and Fundamental Freedoms, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=046. This protocol was ratified by 43 countries including France (in 1974) and Romania (in 1994). It was signed by the United Kingdom in 1953 but never ratified by this country.*

433. *ECtHR, Guide on Article 2 of Protocol no. 4 to the European Convention on Human - Freedom of movement, Council of Europe/European Court of Human Rights, 3 August 2021, n° 101, https://www.echr.coe.int/Documents/Guide_Art_2_Protocol_4_ENG.pdf.*

434. *ECtHR, 3rd Sect., 15 May 2012, FJ Colon v. the Netherlands, appl. n° 49458/06, §3, 98-100, http://hudoc.echr.coe.int/eng?i=001-111347.*

435. *Art. 6 of the EUCFR; art. 5 of the Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 15, as from its entry into force on 1 August 2021, https://rm.coe.int/1680a2353d.*

436. *ECtHR, Guide on Article 5 of the European Convention on Human - Right to liberty and security, Council of Europe/European Court of Human Rights, 31 August 2021, n° 1, https://echr.coe.int/documents/guide_art_5_eng.pdf1.*

437. *ECtHR, Guide on Article 5 of the European Convention on Human Rights, already mentioned, n° 8.*

438. *ECtHR, Guide on Article 5 of the European Convention on Human Rights, already mentioned, n° 10.*

439. *ECtHR, Guide on Article 5 of the European Convention on Human Rights, already mentioned, n° 11.*

440. *ECtHR, Guide on Article 5 of the European Convention on Human Rights, already mentioned, n° 12.*

441. *ECtHR, Guide on Article 5 of the European Convention on Human Rights, already mentioned, n° 13.*

442. *Protocol n°12 the European Convention on Human Rights, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=177. This protocol was ratified by 20 Member States, including Romania (1 November 2006). France and the United Kingdom did not sign it.*

443. *Details of Treaty No. 177, Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=177.*

444. *ECtHR, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention - Prohibition of discrimination, updated on 31 August 2021, n° 7, https://www.echr.coe.int/Documents/Guide_Art_14_Art_1_Protocol_12_ENG.pdf.*

445. *See article 21 of the EUCFR and ECtHR, Guide on Article 14 of the European Convention on Human Rights [...], already mentioned., n° 1.*

446. *ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, appl. n° 53251/13, § 69, http://hudoc.echr.coe.int/eng?i=001-172134.*

447. *ECtHR, Guide on Article 14 of the European Convention on Human Rights [...], already mentioned, n° 28.*

448. *ECtHR, Guide on Article 14 of the European Convention on Human Rights [...], already mentioned, n° 30.*

449. *ECtHR, Guide on Article 14 of the European Convention on Human Rights [...], already mentioned, n° 31.*

450. *ECtHR, Guide on Article 14 of the European Convention on Human Rights [...], already mentioned, n° 31.*

451. *ECtHR, Guide on Article 14 of the European Convention on Human Rights [...], already mentioned, n° 37.*

452. *ECtHR, Guide on Article 14 of the European Convention on Human Rights [...], already mentioned, n° 40.*

453. *Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms n°009, Paris, 20 March 1952, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=009. This protocol has been ratified by almost all the Council of Europe Member States (45 ratifications) including the United Kingdom (1954), France (1974) and Romania (1994).*

454. *Article 14, 1 of the EUCFR; this aspect is not clarified in the Protocol to the ECHR but the ECtHR applies the principle in relation to all categories of schools, for children and adults: see ECtHR, Guide on Article 2 of Protocol n° 1 to the European Convention on Human Rights - Right to education, Council of Europe/European Court of Human Rights, 31 August 2021, n° 12, https://www.echr.coe.int/documents/guide_art_2_protocol_1_eng.pdf.*

455. *FRA, EU Charter of Fundamental Rights, Article 14 - Right to education, https://fra.europa.eu/en/eu-charter/article/14-right-education.*

456. *ECtHR, Guide on Article 2 of Protocol n° 1 to the European Convention on Human Rights, already mentioned, n° 8.*

457. *ECtHR, Guide on Article 2 of Protocol n° 1 to the European Convention on Human Rights, already mentioned, n° 9.*

458. ECtHR, Guide on Article 2 of Protocol n° 1 to the European Convention on Human Rights, already mentioned, n° 10.

459. ECtHR, Guide on Article 2 of Protocol n° 1 to the European Convention on Human Rights, already mentioned, n° 11.

460. ECtHR, Guide on Article 6 of the European Convention on Human rights - Right to a fair trial, Council of Europe/European Court of Human Rights, 30 April 2021, p.7-97, https://www.echr.coe.int/documents/guide_art_6_eng.pdf.

461. Appendix to the Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, 7 November 2007, I (Human Rights and democracy), http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008_CMrec0711_en.PDF.

462. ECtHR, Guide on Article 6 of the European Convention on Human rights, Right to a fair trial, already mentioned, n° 337, referring to ECtHR, 2nd Sect., 19 October 2004, Falk v. the Netherlands, appl. n°66273/01, § 77, http://hudoc.echr.coe.int/eng?i=001-67305.

463. ECtHR, Guide on Article 6 of the European Convention on Human rights, Right to a fair trial, already mentioned, n°379, referring for ex. to ECtHR, plen., 6 December 1988, Barberà, Messegué and Jabardo v. Spain, appl. n°10590/83, § 77, http://hudoc.echr.coe.int/eng?i=001-57429.

464. ECtHR, Guide on Article 6 of the European Convention on Human rights, Right to a fair trial, already mentioned, n° 383, referring to ECtHR, 2nd Sect., 19 October 2004, Falk v. the Netherlands, appl. n°66273/01, § 77, http://hudoc.echr.coe.int/eng?i=001-67305.

465. ECtHR, Guide on Article 6 of the European Convention on Human rights, Right to a fair trial, already mentioned, n° 14, referring to ECtHR, ch., 26 March 1982, Adolph v. Austria, appl. n°8269/78, § 30, http://hudoc.echr.coe.int/eng?i=001-67305.

466. ECtHR, Guide on Article 6 of the European Convention on Human rights, Right to a fair trial, already mentioned, n° 22; outlined in ECtHR, plen., 8 June 1976, Engel and Others v. the Netherlands, appl. n° 5100/71 5101/71 5102/71 (...), § 82-83, http://hudoc.echr.coe.int/eng?i=001-57479.

467. ECtHR, Guide on Article 7 of the European Convention on Human Rights, No punishment without law: the principle that only the law can define a crime and prescribe a penalty, Council of Europe/European Court of Human Rights, 30 April 2021, p. 1, https://echr.coe.int/Documents/Guide_Art_7_ENG.pdf.

468. ECtHR, Guide on Article 7 of the European Convention on Human Rights, already mentioned, n° 48.

469. ECtHR, Guide on Article 7 of the European Convention on Human Rights, already mentioned, n° 6.

470. ECtHR, Guide on Article 7 of the European Convention on Human Rights, already mentioned, n° 8.

471. ECtHR, Guide on Article 7 of the European Convention on Human Rights, already mentioned, n° 11.

472. ECtHR, Guide on Article 7 of the European Convention on Human Rights, already mentioned, n° 12.

473. Declaration CM(2005)56 of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, I.5, http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp.

474. ECtHR, gr. ch., 11 July 2002, Christine Goodwin v. The United Kingdom, appl. n° 28957/95, § 90, http://hudoc.echr.coe.int/eng?i=001-60596; ECtHR, 4th Sect., 8 November 2011, V.C. v. Slovakia, appl. n° 18968/07, § 105, http://hudoc.echr.coe.int/eng?i=001-107364; ECtHR, 4th Sect., 29 April 2002, Pretty v. The United Kingdom, appl. n° 2346/02, § 61, http://hudoc.echr.coe.int/eng?i=001-60448.

475. See Antoine Buyse, 'The Role of Human Dignity in ECHR Case-Law', 21 October 2016, https://www.echrblog.com/2016/10/the-role-of-human-dignity-in-echr-case.html.

476. Article 2 of the ECHR. See ECtHR, gr. ch., 5 June 2015, Lambert and others v. France, appl. n° 46043/14, http://hudoc.echr.coe.int/eng?i=001-155352.

477. Article 3 of the ECHR. See for example ECtHR, gr. ch., 31 January 2019, Rooman v. Belgium, appl. n° no. 18052/11, § 141-143, http://hudoc.echr.coe.int/eng?i=001-189902; ECtHR, 4th Sect., 8 November 2011, V.C. v. Slovakia, appl. n° 18968/07, § 107 and 112-119, http://hudoc.echr.coe.int/eng?i=001-107364.

478. See subsection 4.1.3 of the current study.

479. ECtHR, 5th Sect., 8 October 2020, Aghdgomelashvili and Japaridze v. Georgia, appl. n° 7224/11, § 42, http://hudoc.echr.coe.int/eng?i=001-204815.

480. ECtHR, 4th Sect., 8 November 2011, V.C. v. Slovakia, already mentioned, § 107.

481. ECtHR, 4th Sect., 8 November 2011, V.C. v. Slovakia, already mentioned, § 112.

482. ECtHR, 4th Sect., 8 November 2011, V.C. v. Slovakia, already mentioned, § 119.

483. Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine of 4 April 1997, Treaty n° 164, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=164. The Convention has been ratified by 25 Council of Europe Member States, including Romania (2001) and France (2012). The United Kingdom did not sign it.

484. ECtHR, gr. ch., 4 April 2018, Correia De Matos v. Portugal, appl. n° 56402/12, § 102, http://hudoc.echr.coe.int/eng?i=001-182243.

485. ECtHR, 3rd Sect., 2 June 2020, Tolmachev v. Russia, appl. n° 42182/11, § 51, http://hudoc.echr.coe.int/eng?i=001-202634.

486. ECtHR, 5th Sect., 8 October 2020, Aghdgomelashvili and Japaridze v. Georgia, appl. n° 7224/11, § 49, http://hudoc.echr.coe.int/eng?i=001-204815.

487. ECtHR, 5th Sect., 8 October 2020, Aghdgomelashvili and Japaridze v. Georgia, already mentioned, § 42, http://hudoc.echr.coe.int/eng?i=001-204815.

488. ECtHR, 2nd Sect., 14 January 2020, Beizaras and Levickas v. Lithuania, appl. n° 41288/15, § 117, http://hudoc.echr.coe.int/eng?i=001-200344: "The Court finds it clear that comments on the first applicant's Facebook page […] affected the applicants' psychological well-being and dignity, thus falling within the sphere of their private life. Indeed, the Government acknowledged that those comments had been deplorable for being 'offensive and vulgar' […]".

489. ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, appl. n° 53251/13, § 66, http://hudoc.echr.coe.int/eng?i=001-172134.

490. See the second paragraph of the current subsection.

491. ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, appl. n° 53251/13, § 66, http://hudoc.echr.coe.int/eng?i=001-172134.

492. On the positive obligation to ensure dignity, see for example ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, already mentioned, § 69 and 66: "States had a positive obligation to apply stringent and effective safeguards in order to ensure that their rights to exercise legal capacity were 'practical and effective' rather than 'theoretical and illusory'".

493. See above in the current subsection, in relation to article 28 of the European Convention on Human Rights and Biomedicine.

494. Jeremy McBride, 'Proportionality and the European Convention on Human Rights', in The principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart Publishing, 1999, p. 23 s., p. 25, referring to the court case ECtHR, ch., 25 August 1998, Hertel v. Switzerland, appl. n° 25181/94, § 50, http://hudoc.echr.coe.int/eng?i=001-59366. In the same line, the CJEU verifies whether the interference may «adversely affect the essence of the fundamental right»: CJEU, 8 April 2014, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, § 40, http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12.

495. Sébastien Van Drooghenbroeck and Cecilia Rizcallah, 'The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?', 30 May 2019, German Law Journal (2019), 20, Cambridge University Press, pp. 904-923, p. 907, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/594CA9F2A83DF4B52A1FB6B638339FB4/S2071832219000683a.pdf/echr_and_the_essence_of_fundamental_rights_searching_for_sugar_in_hot_milk.pdf. The authors refer to Janneke Gerards, EVRM Algemene Beginselen, 167 (2011).

496. Antoine Buyse, 'The Role of Human Dignity in ECHR Case-Law', 21 October 2016, https://www.echrblog.com/2016/10/the-role-of-human-dignity-in-echr-case.html.

497. Antoine Buyse, 'The Role of Human Dignity in ECHR Case-Law', already mentioned.

498. On the particular protection that benefits to the right to private life, see for example ECtHR, 1st Section, 6 December 2011, Gladysheva v. Russia, appl. n°7097/10, § 93, http://hudoc.echr.coe.int/eng?i=001-107713

499. Antoinette Rouvroy and Yves Poullet, 'The right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', already mentioned, p. 17, 22 s.; European Data Protection Supervisor, Handbook on European data protection law, 2018, p. 19, https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf: "The right to respect for private life and the right to the protection of personal data […] are thus an essential prerequisite for the exercise of other fundamental freedoms, such as freedom of expression, freedom of peaceful assembly and association, and freedom of religion". See also Fabrice Rochelandet, Il. Quelles justifications à la vie privée ?, in Économie des données personnelles et de la vie privée, 2010, p. 21-37, https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-21.htm?contenu=resume. For the author, the "Enlightenment philosophy implicitly conceives the right to private life as the basis for all civil liberties".

500. Antoinette Rouvroy and Yves Poullet, 'The right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in Serge Gutwirth et al., Reinventing Data Protection?, January 2009, p. 45-76, https://www.researchgate.net/publication/225248944_The_Right_to_Informational_Self-Determination_and_the_Value_of_Self-Development_Reassessing_the_Importance_of_Privacy_for_Democracy, p. 16. See also Fabrice Rochelandet, 'Il. Quelles justifications à la vie privée ?', in Économie des données personnelles et de la vie privée (2010), p. 21-37, https://www.cairn.info/Economie-des-donnees-personnelles-et-de-la-vie-pri--9782707157652-page-21.htm?contenu=resume: "The philosophy of the Enlightenment implicitly conceives the respect of private life as the basis for all personal freedoms" (translated from French). See also Antoine Buyse, 'The Role of Human Dignity in ECHR Case-Law', already mentioned.

501. On the secrecy of private life, see Estelle De Marco, 'The definition of private life', March 2019, publication in the framework of the EU INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, subsection 2.2.1.1.3, https://www.inthemis.fr/ressources/definition-of-private-life.html; Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 12; M. Rudinsky, Civil Human Rights in Russia: Modern Problems of Theory and Practice, Transaction Publishers, 2008, IBSN 978-0-7658-0391-7; Yves Poullet, 'La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ?' in LEGICOM 2009/1 (n° 42), p. 47-69, https://www.cairn.info/revue-legicom-2009-1-page-47.htm.

502. In some circumstances, freedoms such as correspondence and freedom of expression can only be exercised in the "secrecy of private life": see for example Pierre Kayser, La protection de la vie privée par le droit, PU d'Aix-Marseille/Economica, 3rd ed., 1995, p. 11. See also Antoinette Rouvroy and Yves Poullet, 'The right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', already mentioned, subsection 5.1, p. 17.

503. See for example ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, already mentioned, § 66; ECtHR, 1st Section, Gladysheva v. Russia, 6 December 2011, appl. n°7097/10, § 93, http://hudoc.echr.coe.int/eng?i=001-107713: "The right to private life has a "central importance […] to the individual's identity, self-determination, physical and moral integrity, maintenance of relationships with others and a settled and secure place in the community".

504. Antoinette Rouvroy and Yves Poullet, 'The right to

Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', already mentioned, p. 13. See also p. 15-16.

505. *Antoinette Rouvroy and Yves Poullet, already mentioned, p. 13.*

506. *Antoinette Rouvroy and Yves Poullet, already mentioned, p. 14.*

507. *Antoinette Rouvroy and Yves Poullet, already mentioned, p. 1 and 6.*

508. *Respectively in article 1 and in article 2: Antoinette Rouvroy and Yves Poullet, already mentioned, p. 10.*

509. *All these quotations come from Antoinette Rouvroy and Yves Poullet, already mentioned, p. 9. This decision of the German Supreme Court appearing particularly adapted to the topic of the current study, it appears important to quote it almost extensively: "This authority (the possibility for the individual to decide for himself) particularly needs protection under present and future conditions of autonomic data processing. It is particularly endangered because in reaching decisions one no longer has to rely on manually collected registries and files, but today the technical means of storing individual statements about personal or factual situations of a certain or verifiable people with the aid of automatic processing are practically unlimited and can be retrieved in a matter of seconds irrespective of distance. Furthermore, they can be pieced together with other data collection- particularly when integrated information systems are built up- to add up to a partial or virtually complete personality profile, the persons controlled having no sufficient means of controlling its truth and application […]. The possibility of inspection and of gaining influence have increased to a degree hitherto unknown and may influence the individuals' behaviour by the psychological pressure exerted by public interests. Even under certain conditions of modern information processing technology, individual self-determination presupposes that individuals are left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficient certainty which information about himself in certain areas is known to his social milieu and cannot estimate sufficiently the knowledge of parties to whom communication may possibly be made, he is crucially inhibited in his freedom to plan or to decide freely and without being subject to any pressure influence. If someone is uncertain whether deviant behaviour is noted down and stored permanently as information, or is applied or passed, he will try not to attract attention by such behaviour If he reckons that participation in an assembly or a citizens' initiative will be registered officially and that personal risks might result from it, he may possibly renounce the exercise of his respective rights. This would not only impact his chances of development but would also impact the common good ("Gemeinwohl"), because self-determination is an elementary functional condition of a free democratic society based on its citizen's capacity to act and to cooperate".*

510. *Antoinette Rouvroy and Yves Poullet, 'The right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', already mentioned, p. 12.*

511. *Samuel D. Warren and Louis D. Brandeis, 'The right to privacy', Harvard Law Review, vol. IV, 15 Dec. 1890, n°5. See above subsection 4.1.2.1 of the current study.*

512. *See above subsection 4.1.2.2 of the current study.*

513. *Antoinette Rouvroy and Yves Poullet, 'The right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', already mentioned, p. 13. Authors refer to Paul De Hert and Serge Gurtwirth ('Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in Eric Claes, Antony Duff, Serge Gutwirth (eds), Privacy and the Criminal Law, Antwerpen-Oxford: Interscientia, 2006, p. 64: "These rights and liberties enable citizens to develop and exercise their moral powers informing revising and in rationally pursuing their conceptions of the good").*

514. *ECtHR, plen., 8 July 1986, Lingens v. Austria, appl. n° 9815/82, § 42, http://hudoc.echr.coe.int/eng?i=001-57523: "freedom of political debate is at the very core of the concept of a democratic society which prevails throughout the Convention".*

515. *Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', already mentioned, p. 13.*

516. *Antoinette Rouvroy and Yves Poullet, already mentioned, p. 13, see also p. 7.*

517. *In the same line see Paul De Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement: Opacity of the individual and transparency of power', in Erik Claes, Antony Duff and Serge Gutwirth, Privacy and the criminal law, Hart Publishing, 2006, p. 61-102, n° 3.2: "Privacy protects the fundamental political value of a democratic constitutional state as it guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards – for example – their […] behaviour […]. It guarantees each person's uniqueness, including alternative behaviour and the resistance to power at a time when it clashes with other interests or with the public interest".*

518. *ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, appl. n° 53251/13, § 66, http://hudoc.echr.coe.int/eng?i=001-172134.*

519. *Indeed, the ECHR is based on the principle that "fundamental freedoms which are the foundation of justice and peace in the world […] are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which they depend" (preamble).*

520. *On the positive obligation to ensure dignity, see for example ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, already mentioned, § 69 and § 66: "States had a positive obligation to apply stringent and effective safeguards in order to ensure that their rights to exercise legal capacity were "practical and effective" rather than "theoretical and illusory".*

521. *Commission staff working document impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, SWD(2021) 84 final, 21 April 2021, n° 2.1.1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084.*

522. Mélanie Dubuy, 'Le droit de résistance à l'oppression en droit international public : le cas de la résistance à un régime tyrannique', in Civitas Europa, 2014/1 (N° 32), p. 139-163, https://www.cairn.info/revue-civitas-europa-2014-1-page-139.htm.

523. Example of art. 2 of the 1789 French Declaration of Human and Citizens Rights, which considers the right to resist oppression as a natural and imprescriptible right. On this issue see Mélanie Dubuy, 'Le droit de résistance à l'oppression en droit international public : le cas de la résistance à un régime tyrannique, already mentioned, referring to F. Benoït -Rohmer, P. Wachsmann ('La résistance à l'oppression dans la déclaration', Droits, n° 8, 1988, p. 91-99).

524. See above subsection n° 4.1.1 of the current study.

525. Mélanie Dubuy, 'Le droit de résistance à l'oppression en droit international public : le cas de la résistance à un régime tyrannique', already mentioned.

526. Mélanie Dubuy, already mentioned, referring to S. Karagiannis, 'Qu'est-il en droit international, le droit à la résistance devenu ?', RTDH, 2008, p. 949-1005, p. 1003.

527. Mélanie Dubuy, already mentioned. The author refers to E. Lauterpacht (International Law and Human rights, London, Stevens and Son limited, 1950, 475 p., p. 116-117) and J.-J. PAUST ('International law, dignity, democracy and the Arab spring', Cornell International Law Journal, 2013, vol. 46, p. 1-19, note 53) who proposes a list of supporters of this approach, amongst which R. Higgins or A. Cassese.

528. Mélanie Dubuy, already mentioned, referring to R. Kolb ('Autodétermination et 'sécession remède' en droit international public', in The Global community Yearbook of International Law and Jurisprudence, Global trends : law, policy & Justice, Essays in honour of professor Guiliana Ziccardi Capaldi, Oceana, New York, p. 57-77, p. 61).

529. Mélanie Dubuy, already mentioned, referring to J.-J. Paust (The human right to participate in armed revolution and related forms of social violence: testing the limits of permissibility, 1983, 32 Emory LJ 545, 565-6) and J. Morsink (The universal declaration of human rights: origins, drafting and intent, Pittsburgh, University of Pensylvania Press, 1999, p. 308). According to the supporters of this doctrine, the right to resist oppression is inferred by the conjunction of the Preamble of the UN Declaration, which "refers to the rebellion against tyranny and oppression to which the human being is compelled where his or her fundamental rights are not guaranteed" (Mélanie Dubuy, already mentioned), and article 21(3) of the UN Declaration, which states that "the will of the people shall be the basis of the authority of government" (UN Declaration).

530. See the previous subsection of the current study.

531. See subsection 4.1.1 of the current study.

532. Paul De Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement: Opacity of the individual and transparency of power', in Erik Claes, Antony Duff and Serge Gutwirth, Privacy and the criminal law, Hart Publishing, 2006, p. 61-102, n° 3.2.

533. See subsection 4.1.2.5 of the current study.

534. Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', in Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet (dir.), Libertés et droits fondamentaux, Dalloz, 11th ed., 2005, p. 44-45.

535. Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', already mentioned.

536. See also Estelle De Marco, Identification and analysis of the legal and ethical framework, Deliverable D2.2, version 2.2.4 of 12 July 2017, MANDOLA EU project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, especially subsections 3.2 and 4.1.3.

537. See for example Steven Greer, The exceptions to Article 8 to 11 of the European Convention on Human Rights, Human Rights files n°15, Council of Europe publishing, 1997, especially p. 8, http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf; Steven Greer, The margin of appreciation: interpretation and discretion under the European Convention on Human Rights, Human Rights files n° 17, Council of Europe publishing, 2000, especially p. 20 (proportionality); p. 26 (public interest exceptions), http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-17(2000).pdf; Toby Mendel, A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights, Council of Europe, especially p. 3 (freedom of expression), https://rm.coe.int/16806f5bb3; Ivana Roagna, Protecting the right to respect for private and family life under the European Convention on Human Rights, Council of Europe human rights handbooks, Council of Europe, 2012, especially p. 37 (private life), www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf.

538. This aim must be one of those that are listed in the Convention.

539. In a more precise legal wording, it must be "necessary in a democratic society for the aforesaid aim" (1), which implies that the interference, "in a society that means to remain democratic" (2) must correspond to a «pressing social need» (3) and must be "proportionate to the legitimate aim pursued" (4). References: (1) ECtHR, plen., 26 April 1979, Sunday Times v. The United Kingdom, appl. n° 6538/74, § 45, Series A, n° 30, http://hudoc.echr.coe.int/eng?i=001-57584; (2) Joint dissenting opinion of judges Wiarda, Cremona, Thór Vilhjálmsson, Ryssdal, Ganshof van der Meersch, Sir Gerald Fitzmaurice, Bindschedler-Robert, Liesch and Matscher, § 8, available under the Sunday Times court case, already mentioned; (3) (4) ECtHR, Sunday Times v. The United Kingdom, already mentioned, § 59 and § 63 respectively.

540. Article 6, 3 of the Treaty on European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:C2010/083/01&from=FR.

541. The French Constitutional Council recognises the exclusive competence of the Parliament to hold limitations to freedoms, accordingly to article 34 of the Constitution and art. 4 of the 1789 French Human and Citizen Rights Declaration. This Council also considers that the lawmaker "can only limit the exercise of a freedom for a constitutional imperative" (see Frédérique Lafay, note under the Council decision of 18 January 1995, JCP 95, II, 22 525). Furthermore, this council considers that "any restrictions placed on the exercising of (freedoms) must necessarily be adapted and proportionate to the purpose it seeks to

achieve" (see for instance Decision n° 2009-580 DC of 10 June 2009, J.O.R.F. of 13 June 2009, p. 9675, § 15).

542. See for example Decision n° 1258/2009, available in English at http://www.legi-internet.ro/en/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

543. See for example ECtHR, gr. ch., 27 March 1996, Goodwin v. United Kingdom, appl. no17488/90, § 42-43, http://hudoc.echr.coe.int/eng?i=001-57974. The obligation to demonstrate the need for limiting a fundamental right also implies the obligation to demonstrate that divergent opinions were taken into account; see Article 29 Data Protection Working Party, Opinion 01/2014 (WP 211), already mentioned, 3.17-3.19.

544. See for example ECtHR, ch., 26 March 1985, case X. and Y v. The Netherlands, appl. n° 8978/80, § 23, http://hudoc.echr.coe.int/eng?i=001-57603; ECtHR, 3rd Sect., 24 June 2004, von Hannover v. Germany, appl. n° 59350/00, § 57, http://hudoc.echr.coe.int/eng?i=001-61853; ECtHR, Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, already mentioned, p. 4; Antoinette Rouvroy, 'Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence', in Studies in Ethics, Law and Technology, Vol. 2, Issue 1, 2008, Article 3, p. 9, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984.

545. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 27 February 2014, 3.13, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

546. ECtHR, ch., 25 February 1993, Crémieux v. France, appl. n° 11471/85, § 38, http://hudoc.echr.coe.int/eng?i=001-57805. In the same line, see the Opinion of the European Data Protection Supervisor, on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, 26 September 2005, § 10, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2005/05-09-26_data_retention_EN.pdf.

547. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.13.

548. Example of article 8§2 of the ECHR. This notion of legitimate aim is also considered by the Court of Justice of the European Union: see for example CJEU, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, 8 April 2014, § 46, http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12.

549. Article 52.1 of the Charter.

550. Article 29 Data Protection Working Party, Opinion 01/2014 (WP 211), already mentioned, 3.14.

551. Article 29 Data Protection Working Party, Opinion 01/2014 (WP 211), already mentioned, 3.17 - 3.19.

552. The interference must be appropriate to satisfy the identified social need and proportionate to this very need- which is actually the purpose of the interference: see for example Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.17, 3.19.

553. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.13, 3.17, 3.19; ECtHR, plen., 26 April 1979, Sunday Times v. The United Kingdom, appl. n° 6538/74, § 65, https://hudoc.echr.coe.int/eng?i=001-57584.

554. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.19. In the same sense see also CJEU, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, 8 April 2014, § 49, http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12, which verifies whether the interference «is appropriate for attaining the objective pursued».

555. See for example Opinion of the European Data Protection Supervisor, on the Evaluation Report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 31 May 2011, § 41, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf: «statements from Member States on whether they consider data retention a necessary tool for law enforcement purposes» do not «as such establish the need for data retention as a law enforcement measure»; «the statements on the necessity should be supported by sufficient evidence».

556. See for example plen, 22 October 1981, Dudgeon v. The United Kingdom, appl. n° 7525/76, http://hudoc.echr.coe.int/eng?i=001-57473.

557. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.13-3.19.

558. Article 29 Data Protection Working Party, opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism, adopted on 9 November 2004, WP99, p. 4, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf.

559. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned; ECtHR, 5th Sect., 2 September 2010, Uzun v. Germany, appl. n° 35623/05, §51, http://hudoc.echr.coe.int/eng?i=001-100293.

560. Jeremy McBride, 'Proportionality and the European Convention on Human Rights', in The principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart Publishing, 1999, p. 23 s., p. 23.

561. Jeremy McBride, already mentioned, p. 24.

562. Jeremy McBride, already mentioned, p. 24.

563. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.20, referring to ECtHR court cases.

564. ECtHR, 4th Sect., 12 January 2016, Szabó and Vissy v. Hungary, appl. no37138/14, § 73, http://hudoc.echr.coe.int/eng?i=001-160020.

565. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.26: «the more severe the issue and/or the greater or more severe or substantial the harm or detriment which society may be exposed to, the more an interference may be justified".

566. See for ex. ECtHR, ch., 24 February 1997, De Haes and Gijsels v. Belgium, appl. no19983/92, http://hudoc.echr.coe.int/eng?i=001-58015.

567. The ECtHR noted for instance in a court case the lack of consideration of «the nature or gravity of the offence»: Article 29 Data protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.24, referring to ECtHR, gr.ch., 4 December 2008, S & Marper v. United Kingdom, appl. n° 30562/04 and 30566/04, http://hudoc.echr.coe.int/eng?i=001-90051.

568. Jeremy McBride evokes the "proportionality of the very behaviour which is being restricted": 'Proportionality and the European Convention on Human Rights', in The Principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart Publishing, 1999, p. 25.

569. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.26. In order to illustrate the notion of privacy expectation, the working group states «the privacy considerations in terms of context are very different when installing CCTV cameras on a public street as opposed to installing them in toilets or hospital wards».

570. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.24, referring to ECtHR, gr. ch., 4 December 2008, S & Marper v. United Kingdom, appl. n° 30562/04 and 30566/04, http://hudoc.echr.coe.int/eng?i=001-90051; In relation to an obligation to secure one's computer in order to prevent counterfeiting, see Estelle De Marco, 'Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux', 4 June 2009, Juriscom.net, https://juriscom.net/hadopi-analyse-du-nouveau-mecanisme-de-prevention-de-la-contrefacon-a-la-lumiere-des-droits-et-libertes-fondamentaux/.

571. See for example ECtHR, 5th Sect., 19 May 2016, DL v. Bulgaria, appl. n° 7472/14, § 105, http://hudoc.echr.coe.int/eng?i=001-163222. See also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.26.

572. ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, appl. no 37138/14, already mentioned, § 73 and 75-77. On this issue and the previous one see also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.26.

573. On this issue and the previous one, see for example ECtHR, ch., 25 February 1993, Crémieux v. France, appl. n° 11471/85, § 40, http://hudoc.echr.coe.int/eng?i=001-57805.

574. Jeremy McBride, 'Proportionality and the European Convention on Human Rights', in The principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart Publishing, 1999, p. 26. See for ex. ECtHR, gr.ch., 27 March 1996, Goodwin v. United Kingdom, appl. no17488/90, §42-43, http://hudoc.echr.coe.int/eng?i=001-57974. For an application of this principle at the EU level see for example a judgment of the European Union civil service tribunal (first chamber), V. v. European Parliament, 5 July 2011, case F-46/09, § 139, available at http://curia.europa.eu/juris/liste.jsf?language=en&num=F-46/09.

575. Jeremy McBride, already mentioned, p. 26, referring to ECtHR, gr.ch., 27 March 1996, Goodwin v. United Kingdom, appl. no17488/90, http://hudoc.echr.coe.int/eng?i=001-57974.

576. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, n° 3.26.

577. ECtHR, plen., 6 September 1978, Klass and others v. Germany, already mentioned, § 50s.

578. ECtHR, plen., 6 September 1978, Klass and others v. Germany, already mentioned, § 55, referring to "adequate and equivalent guarantees" to be implemented in order to palliate the absence of effective remedy.

579. Ex. ECtHR, plen., 13 June 1979, Marckx v. Belgium, appl. no 6833/74, § 31, http://hudoc.echr.coe.int/eng?i=001-57534.

580. See for example ECtHR, Klass and others v. Germany, already mentioned, § 50-59; see also Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.26.

581. See for ex. Article 29 Data Protection Working Party, Opinion 01/2014, already mentioned, 3.26; ECtHR, 4th Sect., 18 May 2010, Kennedy v. The United Kingdom, appl. n° 26839/05, http://hudoc.echr.coe.int/eng?i=001-98473; ECtHR, 2nd Sect., 24 September 2002, M.G. v. The United Kingdom, appl. n° 39393/98, http://hudoc.echr.coe.int/eng?i=001-60642; ECtHR, Klass and others v. Germany, already mentioned, §. 56.

582. ECtHR, 18 May 2010, Kennedy v. The United Kingdom, already mentioned; ECtHR, 4th sect., 27 October 2015, R.E. v. The United Kingdom, appl. no 62498/11, http://hudoc.echr.coe.int/eng?i=001-158159; ECtHR, gr. ch., 4 December 2015, Roman Zakharov v. Russia, appl. n° 47143/06, http://hudoc.echr.coe.int/eng?i=001-159324.

583. ECtHR, Sunday Times v. The United Kingdom,

appl. n° 6538/74, § 48, https://hudoc.echr.coe.int/eng?i=001-57584: these expressions are «equally authentic but not exactly the same», and are translated by the French expression «prévues par la loi»; the ECtHR must «interpret them in a way that reconciles them as far as possible and is most appropriate in order to realise the aim and achieve the object of the treaty». The expression used in the ECHR is "in accordance with the law". The EUCFR uses the expression «provided for by law» in its article 52§1.

584. *ECtHR, plen., 2 August 1984, Malone v. The United Kingdom, appl. n° 8691/79, § 66, http://hudoc.echr.coe.int/eng?i=001-57533.*

585. *All quotations come from ECtHR, ch., 24 April 1990, Kruslin v. France, appl. no 11801/85, § 29, http://hudoc.echr.coe.int/eng?i=001-57626. On this issue see also Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', in Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet (dir.), Libertés et droits fondamentaux, Dalloz, 11th ed., 2005, p. 43; R. Koering-Joulin, D. 90, chron. p. 187.*

586. *ECtHR, plen., 2 August 1984, Malone v. The United Kingdom, already mentioned: "The expressions in question [are] also taken to include requirements over and above compliance with domestic law"; "the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law […]. The phrase thus implies […] that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities».*

587. *François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 46. See also the preamble of the ECHR.*

588. *On all the aspects developed in the current subsection, see also ECtHR, Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, Council of Europe/European Court of Human Rights, 31 December 2020, n° 563-571, https://www.echr.coe.int/documents/guide_art_8_eng.pdf.*

589. *All quotations come from the European Court of Human Rights case Sunday Times v. The United Kingdom, already mentioned, § 49. See also Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', in Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet (dir.), Libertés et droits fondamentaux, Dalloz, 11th ed., 2005, p. 43; Steve Foster, Human Rights and Civil Liberties, 2nd ed., 2008, p. 464.*

590. *ECtHR, Malone v. The United Kingdom, already mentioned, §67.*

591. *ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, appl. n° 58170/13, 62322/14, 24960/15, § 333, http://hudoc.echr.coe.int/eng?i=001-210077.*

592. *ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, already mentioned, § 333.*

593. *ECtHR, 3rd Sect., 12 May 2000, Khan v. The United Kingdom, appl. no 35394/97, § 26, http://hudoc.echr.coe.int/eng?i=001-58841.*

594. *ECtHR, ch., 24 April 1990, Huvig v. France, appl. no 11105/84, § 32 ("clear, detailed rules"), http://hudoc.echr.coe.int/eng?i=001-57627.*

595. *ECtHR, Malone v. The United Kingdom, §67, already mentioned; ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, already mentioned, § 333.*

596. *ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, already mentioned, § 333. In relation to safeguards, see the following subsection of the current study.*

597. *ECtHR, plen., 26 April 1979, Sunday Times v. The United Kingdom, appl. n° 6538/74, § 49, http://hudoc.echr.coe.int/eng?i=001-57584.*

598. *Ex. ECtHR, ch., 24 April 1990, Huvig v. France, appl. no 11105/84, § 33, http://hudoc.echr.coe.int/eng?i=001-57627.*

599. *Translated from French. French Conseil d'État, 'Sécurité juridique et complexité du droit', already mentioned, p. 282.*

600. *French Conseil d'État, 'Sécurité juridique et complexité du droit', already mentioned, p. 282 and 288. Principles of consistency and intelligibility of legal texts as a whole are most of the time implicit in the ECtHR jurisprudence (see for ex. ECtHR, plen., 2 August 1984, Malone v. The United Kingdom, appl. n° 8691/79, § 66, http://hudoc.echr.coe.int/eng?i=001-57533). However, see ECtHR, ch., 16 December 1992, de Geouffre de la Pradelle v. France, appl. no 12964/87, § 34, http://hudoc.echr.coe.int/eng?i=001-57778; ECtHR, gr. ch., 15 October 2015, Perinçek v. Switzerland, appl. no 27510/08, § 134, http://hudoc.echr.coe.int/eng?i=001-158235.*

601. *ECtHR, Huvig v. France, already mentioned, § 26.*

602. *Translated from French: Pascal Beauvais, 'Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes', in Archives de politique criminelle, ERPC, éd. A. Pédone, 2007/1 (no29), p. 4, https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm.*

603. *Pascal Beauvais, 'Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes', already mentioned, p. 4.*

604. *See for ex. ECtHR, 1st sect., 30 July 2015, Ferreira Santos Pardal v. Portugal, appl. no 30123/10, § 42, f, http://hudoc.echr.coe.int/eng?i=001-156500.*

605. *See for ex. ECtHR, gr. ch., 15 October 2015, Perinçek v. Switzerland, appl. n° 27510/08, § 134, http://hudoc.echr.coe.int/eng?i=001-158235.*

606. *Idem ; French Conseil d'État, 'Sécurité juridique et complexité du droit', already mentioned, p. 281.*

607. *See for ex. ECtHR, 3rd Sect., 1 December 2005, Păduraru v. Romania, appl. n°63252/00, § 98, http://hudoc.echr.coe.int/eng?i=001-71444; ECtHR, Ferreira Santos Pardal v. Portugal, already mentioned, §42.*

608. *ECtHR, 1st sect., 30 July 2015, Ferreira Santos Pardal v. Portugal, already mentioned, §43-49; French Conseil d'État, 'Sécurité juridique et complexité du droit', already mentioned, p. 281.*

609. *French Conseil d'État, 'Sécurité juridique et complexité du droit', already mentioned, p. 281. See ECtHR, ch., 16 December 1992, de Geouffre de la Pradelle v. France, appl. no 12964/87, § 33, http://hudoc.echr.coe.int/eng?i=001-57778; Pascal Beauvais,*

'Le droit à la prévisibilité en matière pénale dans la jurisprudence des cours européennes', in Archives de politique criminelle, ERPC, éd. A. Pédone, 2007/1 (no29), p. 13 s., https://www.cairn.info/revue-archives-de-politique-criminelle-2007-1-page-3.htm; Dominique J. M. Soûlas de Russel, Philippe Raimbault, 'Nature et racines du principe de sécurité juridique : une mise au point', RIDC, 2003, vol. 55, no1, p. 90, referring to ECtHR, plen., 13 June 1979, Marckx v. Belgium, appl. no 6833/74, http://hudoc.echr.coe.int/eng?i=001-57534.

610. *ECtHR, plen., 6 September 1978, Klass and other v. Germany, appl. n° 5029/71, § 50, http://hudoc.echr.coe.int/eng?i=001-57510; See also French Constitutional Council, Decision n° 2013-357 QPC of 29 November 2013, Société Wesgate Charters Ltd, cons. 8, https://www.conseil-constitutionnel.fr/decision/2013/2013357QPC.htm.*

611. *See for example article 15 of the Council of Europe Convention on cybercrime, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.*

612. *See for example ECtHR, Szabó and Vissy v. Hungary, already mentioned, §68, which evokes the "simultaneous development of legal safeguards securing respect for citizens' Convention rights".*

613. *ECtHR, Khan v. The United Kingdom, § 22 s., already mentioned.*

614. *See for ex. ECtHR, plen., 2 August 1984, Malone v. The United Kingdom, § 67, already mentioned; ECtHR, 3rd Sect., 29 June 2006, Weber and Saravia v. Germany, n° 54934/00, § 94, http://hudoc.echr.coe.int/eng?i=001-76586.*

615. *ECtHR, gr.ch., 4 May 2000, Rotaru v. Romania, appl. no 28341/95, § 45 s., http://hudoc.echr.coe.int/eng?i=001-58586.*

616. *ECtHR, Szabó and Vissy v. Hungary, already mentioned, §68.*

617. *ECtHR, plen., 2 August 1984, Malone v. The United Kingdom, § 68, already mentioned; see also ECtHR, 4th Sect., 12 January 2016, Szabó and Vissy v. Hungary, appl. no 37138/14, § 65, http://hudoc.echr.coe.int/eng?i=001-160020.*

618. *ECtHR, 25 May 2021, gr. ch., Big Brother Watch and others v. The United Kingdom, appl. n° 58170/13, 62322/14, 24960/15, § 361, http://hudoc.echr.coe.int/eng?i=001-210077; ECtHR, Klass and others v. Germany, already mentioned, §. 50-56.*

619. *ECtHR, 25 May 2021, gr. ch., Big Brother Watch and others v. The United Kingdom, already mentioned, § 361. French Constitutional Court, decision n° 2004-503 of 12 August 2004, § 29, https://www.conseil-constitutionnel.fr/decision/2004/2004503DC.htm.*

620. *. ECtHR, plen., 2 August 1984, Malone v. The United Kingdom, § 79 already mentioned; French Constitutional Council, Decision n° 2004-503 DC of 12 August 2004, already mentioned, § 29.*

621. *ECtHR, 5th Sect., 2 September 2010, Uzun v. Germany, already mentioned, § 52. See subsection 4.1.2.2 of the current study.*

622. *European Court of Human Rights, Internet: case-law of the European Court of Human Rights, June 2015, p. 10, http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf, referring to ECtHR, plen., 6 September 1978, Klass and others v. Germany, appl. n°5029/71, §49, http://hudoc.echr.coe.int/eng?i=001-57510. See also Article 29 Data Protection Working Party, opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism, 9 November 2004 (WP 99), p.4.*

623. *See subsection 4.1.1 of the current study.*

624. *ECtHR, plen., 6 September 1978, Klass and others v. Germany, already mentioned, §49.*

625. *Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), 3.24, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf, referring to ECtHR, gr.ch., 4 December 2008, S & Marper v. United Kingdom, appl. n° 30562/04 and 30566/04, http://hudoc.echr.coe.int/eng?i=001-90051; E. Court H. R., Klass and others v. Germany, already mentioned, §. 55.*

626. *ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, appl. n° 58170/13, 62322/14, 24960/15, § 336, http://hudoc.echr.coe.int/eng?i=001-210077.*

627. *ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, already mentioned, § 336.*

628. *ECtHR, 4th Sect., 12 January 2016, Szabó and Vissy v. Hungary, appl. no 37138/14, § 73 and 75-77, http://hudoc.echr.coe.int/eng?i=001-160020 (media surveillance); ECtHR, ch., 25 March 1998, Kopp v. Switzerland, appl. n° 23224/94, § 73, http://hudoc.echr.coe.int/eng?i=001-58144 (lawyers surveillance).*

629. *ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, already mentioned, § 337.*

630. *ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, already mentioned, § 337.*

631. *ECtHR, 4th Sect., 12 January 2016, Szabó and Vissy v. Hungary, appl. no37138/14, already mentioned, § 77.*

632. *Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.24, referring to ECtHR, gr.ch., 4 December 2008, S & Marper v. The United Kingdom, already mentioned.*

633. *See for example ECtHR, 2nd Sect., 24 September 2002, MG v. The United Kingdom, appl. n° 39393/98, http://hudoc.echr.coe.int/eng?i=001-60642, and Council of Europe, Case law of the European Court of Human Rights concerning the protection of personal data, 30 January 2013 (DP (2013) CASE LAW), p. 91, http://www.cnpd.public.lu/fr/legislation/jurisprudence/cedh/cedh_caselaw_dp_fr.pdf; ECtHR, Klass and others v. Germany, already mentioned, § 55.*

634. *ECtHR, MG v. The United Kingdom, appl. n° 39393/98, already mentioned; ECtHR, Klass and others v. Germany, already mentioned, § 56.*

635. *See for example ECtHR, Klass and others v. Germany, already mentioned, § 52.*

636. *See for example articles 5 and 6 of the ECHR relating to the right to liberty and security and the right to a fair trial.*

637. *The right to not be subject to torture and degrading treatment is analysed in subsection 4.1.2.11 of the current study. In relation to this right, the ECtHR has established a "severity threshold" which, where crossed, reveals a violation of article 3 of the ECtHR. See for example ECtHR, 5th Sect., 8 October 2020, Aghdgomelashvili and Japaridze v. Georgia, appl. n° 7224/11, § 42, http://hudoc.echr.coe.int/eng?i=001-204815.*

638. *On the adaptation of the requirements for fundamental rights protection to the particularities of freedom of expression see ECtHR, Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, Council of Europe/European Court of Human Rights, December 2011, p. 4, http://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf; Estelle De Marco, Identification and analysis of the legal and ethical framework, Deliverable D2.2, version 2.2.4 of 12 July 2017, MANDOLA EU project - GA n° JUST/2014/RRAC/AG/HATE/6652, subsection n° 4.3.3.1.2, http://mandola-project.eu/publications.*

639. *Jeremy McBride, 'Proportionality and the European Convention on Human Rights', in The Principle of Proportionality in the Laws of Europe, edited by Evelyn Ellis, Hart Publishing, 1999, p 24-25.*

640. *Quotations are issued from Jeremy McBride, already mentioned, p. 24-25.*

641. *ECtHR, ch., 25 August 1998, Hertel v. Switzerland, appl. n° 25181/94, § 50, http://hudoc.echr.coe.int/eng?i=001-59366.*

642. *CJEU, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, 8 April 2014, §40, http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12.*

643. *Quotations are issued from Sébastien Van Drooghenbroeck and Cecilia Rizcallah, 'The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?', 30 May 2019, German Law Journal (2019), 20, Cambridge University Press, p. 904–923, p. 907, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/594CA9F2A83DF4B52A1FB6B638339FB4/S2071832219000683a.pdf/echr_and_the_essence_of_fundamental_rights_searching_for_sugar_in_hot_milk.pdf. The authors refer to Janneke Gerards, EVRM Algemene Beginselen, 167 (2011). See subsection 4.1.2.11 of the current study.*

644. *See subsection 4.1.2.11 of the current study.*

645. *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) (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.*

646. *Article 2 of the GDPR.*

647. *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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC.*

648. *Recital n° 14 of the Directive. See also its article 2.*

649. *Article 29 Data protection working party, Opinion 4/2007 on the concept of personal data (WP 136), 10 June 2007, p. 7, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.*

650. *Article 9 of the GDPR and article 10 of Directive 2016/680 (Processing of special categories of personal data).*

651. *EDPB, Guidelines 3/2019 on processing of personal data through video devices, 10 July 2019, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.*

652. *See for example EDPB, Guidelines 3/2019 on processing of personal data through video devices, already mentioned, n° 72 and n° 132.*

653. *ECtHR, ch., 26 March 1985, case X. and Y v. The Netherlands, appl. n° 8978/80, § 23, http://hudoc.echr.coe.int/eng?i=001-57603; ECtHR, 3rd Sect., 24 June 2004, von Hannover v. Germany, appl. n° 59350/00, § 57, http://hudoc.echr.coe.int/eng?i=001-61853; ECtHR, 4th Sect., 17 Juley 2008, I v. Finland, appl. n° 20511/03, § 37 and 48, http://hudoc.echr.coe.int/eng?i=001-87510; ECtHR, 4th Sect., 2 December 2008, K.U. v. Finland, appl. n° 2872/02, § 42, 46 and 48, http://hudoc.echr.coe.int/eng?i=001-89964.*

654. *2 December 2008.*

655. *Article 5,1, b of the GDPR and article 4, 1, b of Directive 2016/680.*

656. *Article 5,1, c and d and article 6 of the GDPR and article 4, 1, c and d and article 8 of Directive 2016/680 (data must be adequate, relevant, accurate and up-to-date, processing must be "necessary" to the purpose).*

657. *Article 5,1, c of the GDPR and article 4, 1, c of Directive 2016/680, in addition to several other provisions in both texts that are relating to data minimisation.*

658. *Article 35 of the GDPR and article 27 of Directive 2016/680 (Data Protection Impact Assessment).*

659. *Article 9 of the GDPR and article 10 of Directive 2016/680 (Processing of special categories of personal data).*

660. *See for example EDPB, Guidelines 3/2019 on processing of personal data through video devices, already mentioned, n° 72-74 and n° 132.*

661. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic*

communications), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058.

662. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136.

663. See for example European Parliament Think Thank, 'Reform of the e-Privacy Directive', 3 August 2017, https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)608661.

664. Court of Justice of the European Union, Press Release n° 123/20, Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophones and Others, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf, p. 2.

665. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024.

666. CJEU, 8 April 2014, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12.

667. CJEU, Judgment of the Court (Grand Chamber) of 6 October 2020 (requests for a preliminary ruling from the Conseil d'État, Constitutional Court – Belgium, France), Joined Cases C-511/18, C-512/18 and C-520/18, 6 October 2020, https://curia.europa.eu/juris/documents.jsf?num=C-511/18.

668. Court of Justice of the European Union, Press Release n° 123/20, Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, already mentioned, p. 2.

669. Court of Justice of the European Union, Press Release n° 123/20, already mentioned, p. 3.

670. Court of Justice of the European Union, Press Release n° 123/20, already mentioned, p. 3.

671. See subsection 3.1.1 of the current study.

672. For further analysis, see subsection 5.1. of the current study.

673. Commission staff working document impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, SWD(2021) 84 final, 21 April 2021, n° 2.1.1-2.1.4, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084.

674. Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32019R1157.

675. See for example articles 10§1 and 11§1 of the Regulation.

676. See for example article 10§2 of the Regulation.

677. See for example article 10§3 of the Regulation.

678. Recital 21 of the Regulation.

679. Article 3 of the Regulation.

680. Article 10 of the Regulation. See also recitals 21 and 22.

681. In the same line, the CJUE considers that Regulation n° 2252/2004 "does not apply to the use and storage of biometric data for other purposes than issuing a passport. These matters are exclusively within the competence of the Member States. Since the fundamental rights guaranteed by the Charter apply only where national legislation falls within the scope of EU law, the Court could not determine whether the storage and use of biometric data for purposes other than issuing passports are compatible with Articles 7 and 8 of the Charter. It would be for the national courts to assess whether the national measures relating to the use and storage of biometric data are compatible with the ECHR": Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, August 2021, p. 37, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

682. EDPS opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents, 10 August 2018, p. 3, https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf.

683. Statewatch, 'EU: Expanding the Eurodac database: MEPs must put rights first', 8 September 2021, https://www.statewatch.org/news/2021/september/eu-expanding-the-eurodac-database-meps-must-put-rights-first/. See also EDRI, 'Eurodac: Council seeks swift agreement on expanded migrant biometric database', 22 September 2021, https://edri.org/our-work/eurodac-council-seeks-swift-agreement-on-expanded-migrant-biometric-database/.

684. Statewatch, 'EU: Expanding the Eurodac database: MEPs must put rights first, already mentioned.

685. Statewatch, 'EU: Expanding the Eurodac database: MEPs must put rights first', already mentioned.

686. eu-LISA, EURODAC, https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac.

687. Letter sent by several NGOs to members of the European Parliament, Subject: Fundamental rights concerns about the EURODAC reform, 8 September 2021, https://www.statewatch.org/media/2714/

eu-eurodac-open-letter-rights-8-9-21.pdf.

688. Letter sent by several NGOs to members of the European Parliament, already mentioned.

689. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

690. All quotations come from article 1 of the proposed artificial intelligence act.

691. Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, August 2021, p. 30, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

692. Recital n° 33 of the proposed artificial intelligence act.

693. Article 5, d of the proposed artificial intelligence act.

694. Post remote identification is therefore authorised, subject to requirements listed in Chapter 2 of the proposed regulation.

695. Recitals n° 23 and 24 of the proposed artificial intelligence regulation, the latter stating that such processing operations are subject to the application of article 9 of the GDPR.

696. By reference to Article 2(2) of Council Framework Decision 2002/584/JHA 62, and punishable in the member state concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State. See article 5, 1.

697. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, p. 2-3, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

698. See for example subsections 6.1.2, 6.2.2 and 6.2.3 of the current report.

699. See subsection 3.1.1 of the current study.

700. See subsection 4.2 of the current study.

701. See for example Luca Montag et al., The rise and rise of biometric mass surveillance in the EU, EDRi, 2021, https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf. See in particular p. 14 and p. 120. France partly based the creation of its central database by reference to the SIS II legislation, see subsections 3.1.1 and 7.1.2 of the current study.

702. See subsection 7.1.2 of the current study.

703. See subsection 7.1.2 of the current study.

704. EDPB, Guidelines 3/2019 on processing of personal data through video devices, 10 July 2019, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.

705. FRA, Data retention across the EU, 13 July 2017, https://fra.europa.eu/en/publication/2017/data-retention-across-eu.

706. Court of Justice of the European Union, 'Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophones and Others', Press Release n° 123/20, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf, p. 2.

707. See for example Ulrich Sieber and Nicolas von zur Mühlen (eds.), Access to Telecommunication Data in Criminal Justice, A Comparative Analysis of European legal Orders, Max-Planck-Institut für Auslandisches und Internationales Strafrecht, Dincker & Humblot, Berlin, 2016. This publication also details powers of search and seizure.

5

IMPACTS OF THE USE OF MASS SURVEILLANCE TECHNOLOGIES ON HUMAN RIGHTS

5.1 THE SOURCES OF IMPACTS ON 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[706]. This impact may be legally acceptable or not, depending on its context and its characteristics. Consequently, some impacts on human rights (which are also called *"fundamental rights"*, where they are protected by a European or international legal instrument[707]) are legally acceptable, whereas other impacts are not.

In order to be legally acceptable, an impact on a fundamental right must comply with the requirements set-up in the ECHR, in the EUCFR, and potentially further specific legislation that has been adopted in order to enforce the application of these two legal instruments, such as the GDPR or the Police-Justice Directive.

These requirements differ, depending on the fundamental right at stake, since all rights are not protected the same way in the ECHR and the EUCFR. Some fundamental rights are deemed to be absolute and do not suffer any limitation, for example the freedom to hold a belief[708]. Some other fundamental rights are deemed conditional and they can be limited subject to strict conditions specified in the ECHR and by the ECtHR, for example the rights to a fair trial and to liberty[709]. A last group of fundamental rights, which are also deemed conditional, can be restricted following a more general rule which can be summarised in the principles of necessity and of proportionality[710].

Impacts on fundamental rights that comply with the above-mentioned rules are deemed legitimate and, based on the ECHR, lawful. They are inherent in human interactions. Consequently, such impacts must not be condemned.

Impacts on fundamental rights that do not comply with these rules, and primarily the requirements for necessity and proportionality, are deemed arbitrary, and they constitute a violation of the fundamental right that they restrict. They constitute a violation, as such, because they limit a fundamental right in an unnecessary and/or disproportionate way (whether they affect, for example, the right to freedom of choice, the right to free will or the right to confidentiality of information that others – including the state - have no legitimacy to know). This is the case even though the person whose rights are limited does not suffer, spiritually or physically, from this limitation[711]. Indeed, the requirements for necessity and proportionality do not only protect individuals, but also democratic rules and the rule of law, through commanding that everyone respect the rights of others. Antoinette Rouvroy and Yves Poullet emphasise that such respect, when it relates to privacy, enables individuals *"to develop and exercise their moral powers"*, and therefore empowers them *"to participate in the political system"*, thus guaranteeing *"the democratic functioning of society"*.[712]

These illegal impacts are the ones that must be identified and, to the greatest extent possible, prevented or eliminated. The identification of such impacts takes place in two stages.

The first step consists of checking that known practices and legislation comply with the principles of limitation of fundamental rights. We will limit this analysis to compliance with the requirements for necessity and proportionality. Indeed, these requirements 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 turns, offers protection of dignity, self-determination, and a series of other rights such as freedom of expression and the right to not be subjected to discrimination[713].

A necessity and proportionality analysis (which is mandatory under Article 35 of the GDPR, relating to Data Protection Impact Assessment) entails reflection on how to ensure a proper identification of the purposes, the efficiency, and of the minimisation of the initiative or practice which impacts fundamental rights. It also entails identifying the guarantees and safeguards to be implemented in order to secure previous findings.

However, such analysis might not enable the discovery of all potential indirect impacts. For this reason, a second step is dedicated to an analysis of risk to rights and freedoms. This analysis (which is mandatory under art. 32[714] and 35 of the GDPR) aims to identify threat sources (i.e. who or what could impact what we want to protect), threat scenarios (i.e. what can happen, based on an action of this source, and its likelihood) and *"feared events"* (i.e. what we want to avoid, and the severity of an incident, if it occurs). *"What we want to protect"*, in the previous sentence, refers to fundamental rights (which may be called *"primary assets"*) and to the *"supports"* of these fundamental rights, which are the persons, systems, materials or softwares that are involved in the exercise of freedoms (including the components of the initiative under assessment, which will limit these freedoms). For example, the individuals themselves can choose self-censorship, because they fear the existence and results of the data processing, and therefore limit their own rights; police services may control a person based on the findings from data processing, therefore limit his or her right to liberty; a lack of control over an algorithm may drive the data processing to refuse a permission, resulting in limiting a person's freedom of choice or ability to benefit from a service.[715]

Once all threat scenarios and feared events have been identified, together with their likelihood and potential severity, the aim of the risk analysis is firstly to assess the level of each risk that is associated with the activity under evaluation (on a scale which varies, generally, from 1 to 3 or 4). Secondly, the aim of the analysis is to identify the corrective measures that will make it possible to avoid these risks or most of them. Ideally, all risks that appear unnecessary and/or disproportionate should be prevented, as well as risks to freedoms that are absolute, because they constitute a violation of a fundamental right.

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

5.2.1. LACK OF CLARIFICATIONS IN RELATION TO PURPOSES AND THEIR LEGITIMACY

The requirement for necessity implies that the usage of surveillance technology or of biometry pursue a legitimate and determined purpose and is efficient to fulfil this purpose. Consequently, the first step of the analysis consists in assessing the existence of such a purpose[716]. This is of utmost importance, because declared purposes condition all the other results of the analysis.

In this respect, practices in the field, as well as laws and legislative proposals that establish the means of biometric control, show a lack of compliance.

1) LACK OF PURPOSES SPECIFICATION IN RELATION TO PRACTICES

At national levels, the implementation of video-surveillance is not necessarily subject to clear and detailed information.

For instance, in France, websites of city halls do not always inform citizens about the precise purposes of the video-surveillance systems they implement. When they produce information, the latter may also not clarify purposes[717]. Authorisations from the relevant prefecture, which are mandatory for implementing cameras, do not even evoke the purposes that are pursued and just refer to the restrictive list of possible general objectives that are provided for by law[718]. As a result, specific purposes that motivate each surveillance system are not known, which prevents the assessment of the reality of their determination and legitimacy.

The same observation can be made as regards the United Kingdom, where the applicable Code of Practice[719] makes very clear that *"surveillance camera systems operating in public places must always have a clearly defined purpose or purposes in pursuit of a legitimate aim and necessary to address a pressing need (or needs)"*[720]. The Code also highlights that purposes must be determined through the performance of a privacy impact assessment[721].

However, in 2020, the UK Surveillance Camera Commissioner reported that only 50% of local authorities responded to a survey on their compliance with the Code, and that many respondents declared that they did not so far consider being certified in relation to such compliance because *"their processes and procedures"* needed to improve. Overall, this means that transparency is not really ensured towards all video-surveillance systems, in particular in relation to their purposes.[722]

Consequently, a certain number at least of remote surveillance systems, including CCTV systems, do not appear to comply with the principle of legitimate and determined purpose, unless otherwise demonstrated. Such demonstration is the burden of the person responsible for the surveillance system. In addition, the information provided must be easily accessible[723].

2) LACK OF SPECIFICATION OF PURPOSES IN SPECIFIC LEGISLATION

Regarding legislation, we can observe that the specific objectives of surveillance measures established under the legislation are rarely all specified.

For example, Regulation (EU) 2019/1157 justifies the mandatory creation of biometric identity cards by the pursuit of the purpose of *"strengthening the security standards applicable to identity cards"*. However, the regulation authorises states to not suppress the data they collect in order to use them for other purposes, provided that a domestic law is adopted to base such processing in compliance with domestic and EU law[724]. Therefore, the regulation does not specify the purposes for which national biometric identifiers can be collected, whereas it creates the very practical possibility of such collection by member states[725]. Based on a properly conducted privacy impact assessment, a regulation adopted in compliance with the ECHR and EUCFR should have taken into account the high risk it creates and should have identified the necessary corrective measures. The most consistent corrective measure should have been to prohibit the retention of biometric identifiers and to frame this prohibition with supervisory mechanisms, based on the fact that such data collection does not fall within the primary objectives of the regulation. Alternatively, the regulation could have recognised as a purpose the creation of an opportunity, for member states, to collect biometric identifiers, and framed it in order to ensure efficiency and minimisation of personal data processing. In case the PIA would have concluded to a persistent disproportionality, this latter purpose should have been removed, and national data collection prohibited.

In the same vein, the French decree that establishes a national database of biometric identifiers officially pursues the purpose of establishing, delivering, and invalidating identity cards and passports and of preventing and detecting their falsification and counterfeiting[726]. However, it grants access to digitalised facial images, as well as to information such as sex, filiation, eye-colour, email, to – non-exhaustively – law enforcement and specialised intelligence service agents in charge of the prevention and repression of terrorism and threats to the fundamental interests of the nation[727]. Access by these agents to the database has no connection with the management of identity cards. As a result, it should have been considered as another purpose of the law, and declared as such, in order to enable the analysis of its efficiency and proportionality. Further, the purpose of *"prevention and repression of threats to fundamental interests of the nation and of terrorism"* is itself far too broad. Even though it falls within the list of legitimate purposes that may justify a limitation of fundamental rights in the ECHR[728], it

does not respect the requirements for a determined specific and *"pressing"* aim to be pursued in this broader sphere of fighting terrorism and ensuring national fundamental interests.

This, taking into account that the latter notion is a source of various interpretations, which sometimes justify the monitoring of journalists or of human rights activists[729].

In a similar vein, the proposal for an Artificial Intelligence Act invokes the purpose of harmonising rules for the placing on the market, the putting into service and the use of artificial intelligence systems in the Union. In addition, it frames certain practices and prohibits those considered as posing the main risks. However, this act authorises the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes, under strict conditions. Such authorisation implies authorising the implementation of technologies and mechanisms that enable facial recognition to happen, at least after videos have been recorded. As a result, the proposed regulation validates the practical implantation of a very controversial personal data processing[730], which has implications on human dignity[731], without clarifying it in the purposes of the legal instruments, with a view to properly assess its efficiency and proportionality. Once again, a regulation taken in compliance with the ECHR and EUCFR would have made this clarification, or would have absolutely prohibited the facial recognition in public places – in real time or after recording - since this is not covered by the purposes of the legislation.

3) PURPOSES DIVERSION

Written as they are, EU Regulation 2019/1157 and the proposed Artificial Intelligence Act organise diversions of purposes. Indeed, they create on the one hand the practical opportunity for member states to establish biometric databases of all their citizens before any criminal infringement was attempted. On the other hand, they validate the implementation of technologies and mechanisms that enable facial recognition in public places. This is done, respectively, under the guise of strengthening security standards and of harmonising rules relating to artificial intelligence.

In addition, practices show a persistent tendency, from the EU and from its current and former member states, to extend the scope of application of laws once they have been adopted, without accompanying such changes with particularly serious fundamental rights impact assessments. Such scope extension has consequences, in terms of necessity and proportionality, on all the legal provisions and previously implemented legal guarantees against arbitrariness. We may refer in this regard to the progressive extension of the purposes of almost all EU migration legislative acts[732] and of several French ones for the purpose of fighting terrorism and ensuring national security[733]. Such context must be taken into account within the framework of the impact assessment of all measures that lead to limit fundamental rights, in order to anticipate risks that may endanger freedoms in this regard, and in order to implement corresponding safeguards. This is not ensured in the afore-mentioned texts.

Finally, some states established a legal framework that enables a diversion of purpose of almost all the legal instruments that organise peoples' surveillance. Indeed, their penal procedure codes include a provision that enables or commands any public officer, who learns about a penal infringement at the occasion of his or her missions, to inform the public prosecutor about it[734]. This authorises the use, in any kind of penal proceedings, even where the crime is of low severity, of evidence whose collection might have been exclusively authorised in a crucial purpose, such as the purpose of combatting terrorism, as a condition for proportionality of the interference. This legal practice, which contradicts the ECHR and the EUCFR, should be taken into account in the assessment of the proportionality of all legislation aiming at limiting fundamental freedom, possibly to prohibit its application. This is not taken into account in the afore-mentioned texts.

At this stage of the analysis, the three legislative instruments under scrutiny fail the part of the necessity test that relates to determination of purpose.

4) FAILURE TO SPECIFY THE LEGITIMACY OF PURPOSES

The notion of legitimacy refers to compliance with legal principles. These principles primarily include compliance with the list of legitimate objectives that is provided in the ECHR and the EUCFR[735]. In addition, the concept of legitimate purposes refers to purposes that answer a *"pressing social need"*. This expression means that there must be a need

for society to implement the proposed restriction of rights'.[736] Where this need is real, actual and urgent or crucial, restriction of freedoms may be intrusive, even in its nature, in the extent it stays proportionate. Where this need is uncertain, future and/or low, the nature and extent of the restriction of fundamental freedoms must stay low.

Surveillance systems that enable the recording of behaviours of human beings in public places, and even follow their itinerary, in a way that identification techniques, including of a biometric nature, might be applied, in real time or at a later stage, and this, before the commission of any offence, constitute a very high interference with human rights; primarily the right to privacy, to dignity, and to self-determination[737]. The same conclusion can be drawn in relation to the systematic collection of biometric identifiers of the whole population, and in relation to systems aiming to mass monitor behaviours or sounds in order to make and potentially apply decisions to individuals, even as a whole.

Even framed by sufficient safeguards such as short-time data retention and efficient independent control, these measures are very intrusive. As a result, the social need that motivates their implementation must be very high.

Nevertheless, public authorities have not explained, so far, the extent to which these measures are likely to assist in the pursuit of the main purposes that are put forward, namely combatting terrorism and criminal offences and the fight against fraud. Without a clear demonstration of that very need, such intrusive measures should not be implemented.

5.2.2. ISSUES RELATING TO THE PRINCIPLE OF EFFICIENCY

The principle of efficiency is very close to the requirement for legitimacy, but its scrutiny makes it possible to ensure, in practice, that the identified social need is real and actual. This principle requires demonstrating the efficiency of the measure that will restrict freedoms, to satisfy the purpose which is being pursued. It also requires demonstrating that existing measures are no longer sufficient to satisfy this purpose[738].

Regulation (EU) 2019/1157, for its part, justifies the mandatory creation of biometric identity cards by the pursuit of the purpose of strengthening the security standards applicable to identity cards. It evokes the need to fight fraud and falsification (Recital n° 4), to ensure that documents are authentic and to establish the identity of a person (Recital n° 17), such identification being necessary to fight terrorism (Recital n° 6). The impact assessment accompanying the European Commission's proposal evokes, in addition, the interest, for citizens, to set up the framework that might enable them to benefit from electronic services through systems such as eID tackled by the eIDAS initiative[739].

Even though we take these purposes into account, despite the fact that they are not clearly mentioned as such in the legislation, the impact assessment performed by the European Commission does not demonstrate that biometric identification, to the extent and in the way it is imposed, will enable the fight against fraud and terrorism. In particular, it does not demonstrate the practical social impacts of the fraud. It does not demonstrate the added value compared to current methods or to other methods that would not be based on biometry or on such kind of biometry. This demonstration must be done taking into account potentially divergent opinions[740]. In this regards, Edgar A. Whitley and Gus Hosein highlight that *"an ill-informed or poorly implemented policy could potentially make the problem worse rather than better"*[741]. It seems obvious that biometry can ease both the identification of ID cards holders where they cross borders and the use of some electronic services. However, the Regulation's accompanying impact assessment does not demonstrate the extent of the added value of using that kind of biometric authentication in order to enable people to cross borders and use electronic services, compared to other methods already in use. These conclusions are more widely applicable to the EU legislations that establish migration systems[742], which also fail to evidence that the measures they propose tackle the issue efficiently. In this regard, the Article 29 working group observed, in particular, that *"the Entry and Exit System (EES), [involving] the processing of millions of citizens' data, […] will detect over-stayers but not tackle any of the underlying causes and, taken on its own, has no means to reduce the number of over-stayers, other than perhaps functioning as a mild deterrent"*[743].

In the same line, the French Decree that establishes a national database of biometric identifiers[744] does not demonstrate how such database will enable the establishment, delivery, and invalidatation of identity cards and passports, and to what extent its use will be more efficient than other methods that do not imply the constitution of such a database. In relation to the purpose of preventing and detecting falsification and counterfeiting, the comments we made previously, in relation to Regulation 2019/1157, apply. As regards the access of law enforcement and of intelligence services to these identifiers, our previous comments apply as well. No evidence has been brought to demonstrate, as required by the ECtHR[745], that access to such an identity cards database, including a digital facial image, is an efficient means to combat terrorism and threats to national security, and to what extent. In addition, practical societal impacts that would cause a prohibition of such access have not been evaluated, taking into account the views of society and potentially divergent opinions regarding the need to handle such impact. In a related field, the Article 29 Data Protection Working Party noticed, in 2004, that the framework decision on data retention, which proposed a *«comprehensive storage of all traffic data, user and participant data»*, was not accompanied with *«any persuasive arguments that retention of traffic data to such a large-scale extent is the only feasible option for combatting crime or protecting national security»*[746].

This is incidentally the very reason for which the CJUE declared later on that the data retention directive was contrary to the EUCFR[747].

Similarly, in the proposal for an Artificial Intelligence Act, the use by law enforcement agencies of 'real-time' remote biometric identification systems in publicly accessible spaces is not connected to the purpose of harmonising rules for the development and use of artificial intelligence. Therefore, this restriction of rights is inefficient to reach the purpose. If we consider that the legislation also pursues the purpose of combatting crime and threats to internal security, a series of evidences must be provided. Evidence must firstly show that those crimes and threats may be efficiently combatted through remote biometric identification. It must also show the extent of its added value. Evidence must in addition demonstrate the practical social impacts that would be caused by a prohibition of the measure foreseen, taking into account the views of society and potentially divergent opinions regarding the need to handle such impact.

Finally, evidence should contradict the studies that, for example, demonstrate that CCTV surveillance and biometric recognition have a very weak impact in combatting crime.[748] For example, it is reported that, in the United Kingdom, systems have so far *"shown minimal ability in actually leading to arrests, with just two people being arrested in trials in London in which over 25,000 people had their faces scanned by police cameras"*[749]. The public administration specialist Guillaume Gormand evokes, for his part, *«the inconsistent results of a fantasised technology»*[750], after having assessed the Montpellier video-surveillance system.

At this stage of the analysis, we can notice that the three legislative instruments under scrutiny fail the part of the necessity test relating to the efficiency of the interference with fundamental rights. Consequently, they fail the entire analysis based on the *"necessity"* requirement.

5.2.3. ISSUES RELATING TO MINIMISATION

It appears difficult to make an exhaustive analysis of the respect for the principle of minimisation of current laws and practices that organise the possibility of biometrically identifying citizens and residents. Indeed, this requirement must be assessed taking into account the purposes, the efficiency, and the added value of legislative provisions and practices, which the states and the European Union failed to demonstrate. In particular, this requirement implies the need to identify the data that is necessary in relation to each purpose[751].

However, even without this information, it seems very challenging to sustain that the proposed personal data processing operations do not go *«further than needed to fulfil the legitimate aim being pursued"*[752], and, in particular, that they are strictly necessary, both for the *"safeguarding of the democratic institutions and [...] for the obtaining of vital"*[753] information in relation to their purposes.

Indeed, before these legislations, the management of national identity cards, the offer of electronic services, the possibility to cross borders, the existence of security standards, and the combat against terrorism and national security threats were already effective. In contrast, the measures at stake

concern the whole population, before any prohibited action has been attempted, based on the processing of personal data that is among the most sensitive, along with DNA. Indeed, biometric data constitute super universal identifiers, which may be both of a highly identifying nature and highly irrevocable, in the sense that they may be irremediably linked to a person – even though they are not insulated from usurpation[754]. As a result, if biometry is implemented in order to ensure a precise match[755], any control, whether arbitrary or justified, based on real facts or on a computer-based classification subject to approximations and errors[756], or even based on the collection of an evidence deliberately created after a theft[757], makes it possible to identify with certainty a unique natural person, which will neither be able to deny that the biometric data designate them, nor to change such data within the framework of their futures activities. This, taking into account that controls might be operated remotely and thus might be, in practice, invisible.

Consequently, there is an apparent but clear imbalance between the purposes that are put forward, which appear likely to be reached through the implementation of alternative measures, and the seriousness of the interference with human rights. This interference impacts primarily the right to private life, to intimacy, to self-determination, and to dignity[758]. Moreover, behavioural recognition technology may impact the right to non-discrimination[759], the right to hold a belief (which is an absolute right), and the right to a fair trial, in cases where a technological decision would reverse, in practice, the burden of proof[760]. In addition, remote biometric identification might impact the right to resist oppression, freedom of movement, and the right to manifest an opinion.[761]

In such a context, current practices that constitute such interference must be stopped, until deeper analysis of their added value for society as a whole. This analysis must establish that there is a crucial and urgent need to create such restriction of fundamental rights, taking into account an established higher interest to do so and an equally demonstrated absence of any weakening of the democratic institutions on that occasion[762]. This must be based on an effective debate provoked at national levels in order to gather citizens' opinion, as it is ordered by the Council of Europe Convention on Human Rights and Biomedicine[763]. This must be done bearing in mind that, according to article 2 of the latter Convention, *"the interests and welfare of the human being shall prevail over the sole interest of society or science"* and that several legal authors, together with the ECtHR, clarified that *"the mere existence of new technologies is far from being a sufficient reason for them to be used"*[764].

It is worth reminding that the EDPS itself asked to *"reassess the necessity and the proportionality"* of the proposal for the regulation on biometric identity cards[765], even though its opinion has not been taken into account. In the same line, the EDPB and the EDPS, in their joint opinion that calls *"for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces"*[766], put forward the *"high-risk of intrusion into individuals' private lives, with severe effects on the populations' expectation of being anonymous in public spaces"*. Based on the same reason of disproportionate interference with individuals' fundamental rights, these data protection authorities also recommend a ban *"on AI systems categorizing individuals from biometrics into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination"* and a prohibition of *"the use of AI to infer emotions of a natural person"*[767].

At this stage of the analysis, it appears that all the practices and texts under scrutiny fail the test of necessity and proportionality.

5.2.4. ISSUES RELATING TO THE PRINCIPLE OF LEGAL BASIS AND TRANSPARENCY

As seen previously in the current study, interferences with freedoms must be established on a legal basis, such notion referring to a law or other legal instrument that complies with domestic and international law.[768]

1) LACK OF APPROPRIATE LEGAL BASIS

The legal basis establishing restrictions of freedoms must comply with relevant national and international legislation. However, this does not appear to be the case in relation to both the EU legislation and some national legislation under scrutiny.

Indeed, Regulation 2019/1157 on strengthening the security of identity cards declares itself[769] to be based on article 21 of the Treaty on the functioning of the European Union (TFEU)[770]. However, this article does not cover the provisions that impose biometric identifiers in identity cards. Likewise, it does not cover the provisions that organise the practical possibility, for member states, to collect such identifiers.[771]

The proposal for a regulation on artificial intelligence declares itself to be based on article 114 TFUE and article 16 TFUE.[772] However, article 114 does not cover the possibility to authorise member states to use biometric technologies in public areas. In the same line, article 16 appears not to be appropriate because the protection of personal data is not *"one of the essential aims or components of the rules adopted by the EU legislature"*, as highlighted by the EDPB and the EDPS[773]. Worse, the proposal for a regulation does not organise a personal data protection. On the contrary, it does authorise the use of artificial intelligence technologies which are currently not allowed, unless it is demonstrated that they comply with the provisions of the ECHR, of the EUCFR, and of the GDPR or the Police-Justice Directive. In addition, the proposal for a regulation does not clarify whether the GDPR and the Police-Justice Directive apply to the provisions it introduces. Finally, this proposal does not organise independent oversight in situations other than 'real-time' remote biometric identification in publicly accessible space for LE purposes.[774]

At national levels, in democratic societies governed by the rule of law, the parliament should be the only legitimate authority that can adopt, after proper debate, provisions that imply high risks for fundamental rights and civil liberties. Member states that use regulatory acts, in order to establish the processing of biometric identifiers or mass surveillance technology, circumvent such parliamentary authority. For example, in France, the national biometric database has been set up by a decree[775], whereas article 34 of the French Constitution grants to the parliament the power to determine *"rules relating to criminal procedure and fundamental guarantees granted to citizens for the exercise of civil liberties"*.

2) LACK OF EFFECTIVENESS OF PARLIAMENTS DECISION-MAKING POWER

Adopting a law in compliance with democratic rules implies that law is discussed and adopted by a parliament with effective decision-making power[776], in countries where the Constitution grants such institution with the legislative authority. Any circumvention of this rule should be temporary and duly justified.

However, in some countries, the powers of parliament are undermined by several mechanisms which are often related to separation of powers. For instance, in France, the lawyer Fran ois Sureau explains that the establishment of the five-year presidential mandate has suppressed, in practice, the opportunity of a parliamentary opposition[777]. The situation is worsened by the growing habit, analysed in the previous subsection, of circumventing parliament by means of regulatory acts that are adopted without democratic debate.

Disregarding the opinion of legitimate authorities

Either way, whether provisions are adopted by the government or by the parliament under the impulse of the latter, 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[778] and at the EU level[779]. This is a worrying situation, because it means that governments and European Institutions do not respect the counter powers that have been established in order 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. And indeed, Fran ois Sureau shows that the executive disregard of counter power is also likely to prompt parliamentary members to adopt proposed laws in order to avoid to be deprived from the possibility to discuss further laws of the same kind if they would raise an opposition[780]. In addition, this favours the proliferation or modification of legal texts, which undermines legal clarity and certainty.

We can, for example. note that before Regulation 2019/1157 on strengthening the security of identity cards was adopted, the EDPS recommended *"to reassess the necessity and the proportionality of the processing of biometric data (facial image in combination with fingerprints)"*[781] before adopting such a measure. This recommendation has been ignored.

The EDPS also recommended that the proposal *"explicitly provides for safeguards against Member States establishing national dactyloscopic databases in the context of implementing the Proposal"*, clarifying that *"a provision should be added […] stating explicitly that the biometric data processed in its context must be deleted immediately after their inclusion on the chip and may not be further processed for purposes other than those explicitly set out in the Proposal"*[782]. This recommendation was also not transcribed in the adopted regulation.

Previously, the EDPS criticised the access granted to law enforcement to the EURODAC[783] systems but its opinion was not taken into account.

Another example of the tendency to disregard contrary opinions from legitimate authorities is given by the French decree that organises the constitution of an ID cards database including biometric identifiers. This decree was adopted after the French Constitutional Council considered unconstitutional a previous law that was trying to create this very same database. The Constitutional Council observed that *"taking account of the nature of registered data, of the scale of the processing, of the latter's technical characteristics and of the conditions set-up for its consultation, [the submitted provisions] interfered with the right to private life in a manner that cannot be considered as proportionate to the aim pursued"*[784]. The government managed to ignore this prohibition.

The proposal for an Artificial Intelligence Act is still under discussion, but we can note that, at this stage, several voices called for either a demonstration of the necessity and proportionality of the use of biometric recognition technologies in public spaces, or for a general prohibition of such technologies. Beyond the NGO campaign in that sense[785], these voices include the EDPB and the EDPS[786], as well as members of the European Parliament, on an individual basis[787] and collectively. In a press release dated 29 June 2021, the members of the European Parliament call for safeguards *"against mass surveillance"* in the context of *"the use of Artificial Intelligence in law enforcement and the judiciary"*, including a *"permanent ban on the use of biometric details like gait, fingerprints, DNA or voice to recognise people in publicly accessible spaces"*. They also state that *"facial recognition should not be used for identification until such systems comply with fundamental rights"*[788].

Reversal of ECHR and EUCFR values

Parliamentary opposition, and more widely citizens' opposition, is further weakened by the form of communication[789] which has been employed by public authorities for at least two decades[790], as already evoked previously in the current study[791]. This communication indeed promotes security at the top of freedoms[792] while security should be presented as an exception to freedom[793]. At the same time, the use of highly questionable assertions stigmatises the persons who question the legitimacy of public authorities to access their personal data[794], which does not make it possible to set the terms of objective debate.

In addition, oral and legal statements very frequently use a vocabulary that presents interferences with rights as measures protective of these very rights.

For example, Regulation 2019/1157 on strengthening the security of identity cards declares that its first aim is to *"facilitate the free movement of persons while ensuring the safety and security of the peoples of Europe, by establishing an area of freedom, security and justice"*, whereas it organises the possibility to seriously interfere with all EU citizens' and residents' private life and dignity before any beginning of execution of a criminal offence[795].

The proposal for a regulation on artificial intelligence[796] declares that it aims at enhancing *"governance and effective enforcement of existing law on fundamental rights and safety"* whereas it organises the possibility to use biometric identification on any EU citizen and resident in public places.

The impact assessment that accompanies the proposed artificial intelligence act seriously assesses risks to a series of fundamental rights[797]. However, the proposal itself merely welcomes the fact that restrictions posed to the freedom to conduct business and to the freedom of art and science, *"when high-risk AI technology is developed*

and used", are *"proportionate and limited to the minimum necessary to prevent […] infringements of fundamental rights"*[798]. Such assertion reverses the value of freedoms since the right to private life supersede in this case the freedoms to conduct a business and the freedom of art and science[799].

At the national level, we can observe that the French law establishing a national database including biometric identifiers, and declared unconstitutional in 2012, was named *"law relating to the protection of identity"*[800].

All the above-mentioned acts demonstrate that actual stakes are not appropriately taken into account. Further, their terms leave the impression that their real actual objective is to give to states the means to monitor citizens, while using a rhetoric that aims to make this objective acceptable. In this respect, a specialist of the topic noted, in 2006 already, that risks to fundamental rights *"are reinforced by the objective of interconnection of the whole of security files at the European level"*[801].

These considerations might appear beyond the topic of the discussion but they are of utmost importance in a context where democratic guarantees against arbitrariness can only be established by laws that are adopted in the respect of democratic rules. Where the latter rules are disregarded, legal provisions adopted in that context cannot be assumed to be proportionate. This leads to call for a moratorium in relation to the establishment of most sensitive interference with human rights, such as the collection and the use of biometric identifiers concerning all EU citizens and residents, for the time required to both conduct an effective assessment of the democratic functioning of EU institutions and of its member states, and to draw conclusions relating to what must be implemented in order to correct this situation.

5.2.5. LACK OF OTHER GUARANTEES

Guarantees and safeguards aim to establish a framework that ensures that the decisions that have been made in order to ensure the necessity and the proportionality of a restriction of freedoms will happen.

An indispensable guarantee is transparency. This transparency must be binding on the person, institution or authority that implements the restriction of freedoms. Transparency must also ensure foreseeability for citizens. For these reasons, transparency must be primarily ensured in the law.

This implies that the law must clearly define the scope and manner of exercise of limitations of rights, including the grounds and circumstances that may base their authorisation, the procedures to be followed to authorise and implement them, the limits of the power, especially in terms of duration, as well as the procedures and modalities for effective supervision of compliance with these safeguards, by an independent authority, at several stages, from the decision to recourse to the measure that will interfere with rights, to the termination of such measure.[802]

LACK OF TRANSPARENCY OF PRACTICES

However, in relation to video-surveillance, we noticed that information is often missing in relation to the purposes pursued. Other information relating to surveillance operations is also often missing, for example in the United Kingdom and in France[803].

LACK OF SAFEGUARDS IN LEGISLATION

In EU regulation 2019/1157 as well as in the proposed Artificial Intelligence Act, proposed guarantees are globally insufficient.

For example, Regulation 2019/1157 only prohibits the storage of biometric identifiers for more than 90 days. It does not exclude their storage for other purposes, and it simply refers to national law for the determination of such purposes.

Similarly, the proposal for an artificial intelligence act only frames the use of 'real time' remote biometric identification in publicly accessible space for LE purposes. It simply refers to national law for usage that would be posterior to a recording, as well as for usage for intelligence purposes.

In addition, neither of these legal instruments provides for guarantees that national data protection authorities will have the effective powers and capability to supervise such interferences with fundamental rights.

Similar conclusions may be drawn in relation to border management and cooperation policies. In particular, it appears that they do not properly ensure the security of the Schengen Information System, which gathers biometric information on several categories of persons, such as missing persons or irregular migrants.[804]

This takes place in a context where, more generally, the powers granted to the public authorities at national levels, in their prevention and surveillance missions, are increasing but are rarely appropriately framed[805] in relation to their definition and scope[806]. To this we can add that certain practices are not disclosed. Their opacity appears to be organised by intelligence services themselves[807], where it is not due to classification as a defence secret[808].

LACK OF EFFICIENCY OF LEGAL REMEDIES

Moreover, the issue of the efficiency of legal remedies against the powers of law enforcement agencies and intelligence services, before courts and other legitimate institutions such as data protection authorities, can be legitimately raised. Indeed, the decisions of these authorities are chronically not followed or fulfilled by executive authorities, which regularly maintain or reintroduce legislative proposals that have been ruled contrary to the Constitution or to the ECHR.[809] This issue might command in itself a debate, at the EU level, on the ways of giving back to these authorities the powers they are owed in a democratic society governed by the rule of law.

Consequently, practices and European legislation under scrutiny do not appear *"to give the individual adequate protection against arbitrary interference having regard to the legitimate aim of the measure in question"*[810]. They also do not appear to exclude any *"obscurity and uncertainty as to the state of the law"*[811]. We can draw the same conclusion in relation to the French decree that establishes a national biometric database. Indeed, this decree has been adopted after the French Constitutional Council considered unconstitutional a previous law with similar provisions, for lack of proportionality and safeguards.[812]

This conclusion is also the one drawn by several legal authors. For example, Sylvia Preuss-Laussinotte shows that, in relation to personal data processing activities for the purpose of security, *"the European Union made the choice to place this question from a perspective of respecting fundamental rights. But [this protection], in practice, appears very formal and ineffective […]. That comes in addition to a series of unsolved technical dysfunctions and to issues raised by the conversion of biometric data into real public data, stored in a considerable number of computing systems"*[813].

5.2.6. CONCLUSION OF THE NECESSITY AND PROPORTIONALITY ASSESSMENT

All the practices and legislation that we analysed fail the analysis of necessity and proportionality. This means that they violate fundamental freedoms, at least the rights to private life and to personal data protection. As such, they are contrary to the ECHR and to the EUCFR.

AT THIS POINT, IT IS WORTH RECALLING THE FOLLOWING STATEMENT FROM THE ECTHR:

"The Contracting States [do not] enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[814]

Indeed, *"the mere existence of new technologies is far from being a sufficient reason for them to be used"*[815]. If guarantees of necessity and proportionality cannot be given, the practices under scrutiny must be stopped, and the legislation that bases them must be repealed. This concerns at least the collection of highly identifying biometric data, and biometric and behavioural recognition in publicly accessible places.

5.3 RISKS FOR HUMAN RIGHTS

5.3.1 RISKS FOR THE RIGHT TO PRIVATE LIFE

1) DISPROPORTIONATE LOSS OF OPACITY FOR THE INDIVIDUAL

The first impact of the use of mass surveillance technology is a restriction of the right to live *"away from unwanted attention"*[816]. Indeed, opacity of the individual[817] is also protected in publicly accessible places, to the extent that no other right or interest imposes a necessary and proportionate restriction of confidentiality[818]. Legitimate restrictions include, non-exhaustively, those needed for interacting with other human beings, and those needed for preventing and repressing offences (which must also be necessary and proportionate in their definition). The necessity and proportionality of these restrictions are supposed to be ensured by applying national law, which transcribes these principles into specific rules. For example, civil codes generally provide for civil liability in case of fault or neglect, and procedure penal codes frame the powers of police services.

The latter procedural legal framework provides for one particular rule which is of utmost importance: the prohibition on restricting freedoms before a prohibited action has been, at least, initiated. Exceptions to this rule must be particularly justified, temporary, and framed.

As a result, a permanent surveillance of public places, before any offence has been initiated, is, as such, a violation of the right to private life since it cannot be justified. The ECtHR recalled many times that surveillance is prohibited *"where there is no link between the conduct of the persons whose data are affected and the objective pursued by the legislation at issue"*[819]. This covers indiscriminate video-surveillance. This covers a fortiori any initiative that would lead to follow the tracks of a person in several places, or to remotely identify a person using biometric identifiers, in real time or after recording.

This also covers the general and indiscriminate retention of biometric identifiers, relating to all citizens and residents. Where biometric identifiers are of a high quality, they enable to identify individuals *"with precision in a wide range of circumstances"*.[820] Consequently, their *"blanket and indiscriminate"* collection, by public authorities, in relation to persons who are not under investigation or convicted of offences, constitutes a violation of the right to private life, and it *"cannot be regarded as necessary in a democratic society"*.[821] The ECtHR issued this decision in relation to the fingerprints of former suspects of offences. It is undoubtedly also applicable to fingerprints and to identifiers that enable facial recognition, relating to the whole population of a country or relating to all migrants. Indeed, migration cannot be considered as an offence since it is protected under the right to freedom of movement.

No argument can be put forward against this rule in a political democracy governed by the rule of law. Especially, internal security is not a sufficient justification.[822] The existence of technology is also not a justification. In this respect, the ECtHR recalled that *"the use of modern scientific techniques cannot be authorised at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests"*[823].

2) UNJUSTIFIED LOSS OF PERSONAL DEVELOPMENT AND OF PERSONAL AUTONOMY

Surveillance also impacts the rights to personal development and to personal autonomy. Indeed, individuals who feel they are being monitored may have a tendency to censor themselves.[824] They might, as a result, not behave as they would have preferred behaving, especially for fear of engaging in behaviour which might be perceived as deviant[825]. They also may avoid meeting another person in a monitored 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. The impact exists per se, insofar as it creates the possibility for self-censorship.[826] Such impact is higher than the impacts caused by online surveillance[827], because surveillance in public places is more difficult to circumvent[828]. It is not permissable in a democracy governed by the rule of law, if not necessary, proportionate, and duly justified. These requirements especially imply that the conduct of each person that is likely to be monitored has a link with the purpose of the legislation that motivates the first monitoring action (such as video-surveillance)[829], and that the surveillance operation is of short duration.

3) GENUINE, CURRENT AND SERIOUS THREAT TO SELF-DETERMINATION AND TO DIGNITY

Moreover, *"visual and acoustical surveillance"*, as well as the collection and the processing of biometric identifiers, impacts the right to physical and psychological integrity, as well as the rights to self-determination and to dignity.

Data collected through visual and acoustical surveillance, as well as biometric characteristics that are used to categorise people or to anticipate peoples' behaviours, relate both to the human body and the human mind. Consequently, they may disclose an important number of *"information on a person's conduct, opinions or feelings"*[830], which are very intimate and which may further be biased. Biometric identifiers such as facial templates and fingerprints relate to the human body and are, by nature, highly intimate.

Taking into account their highly intimate nature, these categories of data particularly carry the risk, where processed, of amounting to *"a 'datafication' of humans"*[831], which entails several possible impacts.[832]

A first possible impact, for the person concerned, is the risk of being treated with a lesser level of respect, compared to situations where decisions are made outside any personal data processing. Indeed, decisions are, in such cases, firstly made on data and not on individuals[833]. In this line, Christiane Wendehorst and Yannic Duller observe that, according to Anton Alterman, *"the use of objectified characteristics of humans for identification purposes by others is viewed as a contradiction to Kant's fundamental principle that people are to be treated as ends in themselves, never merely as a means"*.[834] The processing of such intimate information may therefore wound the dignity of people concerned, thus impact them psychologically.

Another possible impact, for the person concerned, is the risk of being subjected to an illegitimate decision, without any possibility of escape[835]. Indeed, as previously evoked[836], biometric identifiers, where they are implemented in order to ensure a precise match (or where they are considered as such, rightly or wrongly[837]), are super universal identifiers, in the sense that they are both of a highly identifying nature and highly irrevocable. Consequently, any control enables the identification of a natural person with certainty. This person will neither be able to deny that the biometric data designate him or her, nor to revoke such data for the future. This, taking into account that any kind of control is conceivable, whether arbitrary or justified, based on real facts or on a computer-based classification subject to approximations and errors, or even based on the collection of an evidence willingly created after a theft[838]. Moreover, controls might be operated remotely and thus be, in practice, invisible.

Biometric data, insofar as it may be used by a third party including a state, represent therefore a genuine, current and serious threat to the right to self-determination and to human dignity. Both these rights suffer no limitation in a democracy governed by the rule of law[839].

5.3.2 RISKS FOR THE RIGHT TO FREEDOM OF EXPRESSION AND OF ASSEMBLY

The right to self-determination that is protected under the right to private life enables the exercise of other freedoms, such as the freedoms of expression and of assembly.

In this respect, Yves Poullet raises the following issue: *"Can we envision a true freedom of expression where everybody feels they are being watched in relation to their choice and activities?"*[840].

Indeed, disproportionate surveillance may induce self-censorship, as shown by the EDPB: *"The*

intensive use of video devices has an impact on citizen's behaviour. Significant implementation of such tools in many spheres of the individuals' life will put an additional pressure on the individual to prevent the detection of what might be perceived as anomalies. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services and generally limit the possibility of remaining unnoticed."[841]

We previously analysed[842] that the risk of self-censorship is sufficient, per se, to observe an interference with the right to freedom of choice, of expression or of assembly, where it is based on the processing of personal information. This being said, this impact has also been shown to happen in practice. In relation to online surveillance, the Council of Europe reports that, in 2013 and after NSA surveillance had been exposed, 28% of American residents who answered a survey declared that they *"curtailed or avoided social media activities"*. The Council of Europe further reports that, amongst people who were interviewed, *"24% have deliberately avoided certain topics in phone or e-mail conversations; and* 16*% have avoided writing or speaking about a particular topic"*.[843]

Self-censorship is a kind of impact on the right to self-determination, because it impacts individuals' behaviours. It might be induced by any kind of massive surveillance, including video-surveillance.[844] This is all the more the case with biometric surveillance. Incidentally, such behaviour impact is even one of its objectives, at least in the eyes of some public representatives[845].

Consequently, facial and behavioural recognition in publicly accessible places may impact the right of assembly and association. This has been shown by the German Supreme Court, which stated in a 1983 decision that *"those who count with the possibility that their presence at a meeting or participation in a civil initiation be registered by the authority will be incited to give up practising their basic rights"*.[846].

Facial and behavioural recognition in publicly accessible places also impacts, in theory and in practice, the right to freedom of expression. It is worth recalling that freedom of expression is an *"essential foundation"*[847] of democracy and the rule of law and *"one of the basic conditions for its progress"*[848]. This approach is also the one of the EU, which can be summarised by quoting the EU Parliament: *"freedom of expression in the public sphere has been shown to be formative of democracy and the rule of law itself, and coaxial to its existence and survival"*[849]. Consequently, states have a positive obligation to ensure the effectiveness of these rights, which implies giving citizens the confidence that they can express themselves without fear[850]. This implies, in particular, to not monitor individuals where not duly justified, necessary and framed, including a limitation in time. This also implies, for public authorities, to not communicate in a way that stigmatises the persons who carry contrary opinions.[851]

5.3.3 RISKS FOR THE ABSOLUTE RIGHT TO HOLD A BELIEF

It is reported that some advanced technology, called *"brain computing-interfaces (BCI) […] measure neuro activity and translate brain activity into machine readable input"*. These might allow *"the detection of thoughts or intent and possibly also [influence] operations of the human brain"*.[852]

More generally, several technologies are developed in order to identify or infer *"emotions, thoughts or intentions of natural persons on the basis of bio-signals"*[853]. Several experiments have especially been documented[854].

These technologies may have an impact on individual thoughts, by manipulating them or by inducing self-monitoring. Such impact, based on the processing of personal data, contradicts the right to hold a belief, which is an absolute right[855].

Consequently, these technologies cannot be used without informed consent of the people concerned. This requirement is applicable to the pursuit of internal security purposes as well as to the prevention and repression of criminal offence. Indeed, states are bounded to the respect of the ECHR.

5.3.4 RISKS LINKED TO ERRORS AND THEFT

Biometric systems are liable to errors. In addition, biometric identifiers are susceptible to theft. These situations induce a number of impacts on fundamental rights.

1) TECHNOLOGY-BASED ERRORS

Bernadette Dorizzi[856] explains that biometric systems are subject to two types of errors. The first one, called *"false match"*, leads the system to falsely recognise or authenticate a person (in this latter case, it is called *"false acceptation"*). The second one, called *"false non-match"*, leads the system to not recognise or not authenticate a person, where it should[857]. Depending on the quality of the identification system implemented, errors may occur at a significantscale. In this respect, several authors argue a frequent failure to seriously assess technology risks[858]. In particular, Edgar A. Whitley and Gus Hosein explain that, at the EU and the UK level, *"not a single feasibility study or technology study was introduced to inform parliamentarians about the advantages, disadvantages, or potential failure […]. The common view […] was that because the technology was approved by UN bodies […]. The ICAO did not scrutinize the technology in detail either, however. [One of its members] admitted that […] they were unsure of the abilities of the technology to match their goal"*. Authors conclude that policies are *"never adequately reviewed at any level as each level presumes that the other level will or has done it"*.[859]

In addition to these weaknesses, it is worth noticing that the efficiency of biometric recognition is not the same depending on the colour of the skin[860] and its potential imperfections (such as in case of skin disease)[861].

A striking example of errors due to false match is provided by an independent report, from an expert on surveillance at Essex University. The report concludes that the facial recognition system used by the London Metropolitan Police is *"verifiably accurate in just* 19*% of cases"*[862], which means that *"*81*% of 'suspects' flagged by [the] technology [are] innocent"*[863].

2) HUMAN BASED ERRORS AND WEAKNESSES

A set of technology is developed with the aim of evaluating or classifying natural persons, based on their physical characteristics or their behaviours, in a variety of purposes. These purposes include the evaluation of people's personalities and trustworthiness[864].

The construction of the categories used[865], as well as the way the technology processes these categories, is human-based and subjective. As a result, errors may arise.

The way in which technology is implemented may itself lead to unpredicted and unwanted impacts. Especially, it may *"reinforce race or ethnic stereotypes"*[866] as well as any other kind of stereotype. For example, if a particular population is more represented than another in the biometric database, there is a chance that the number of positive matches will be higher in relation to that population, thus leading to *"negative discrimination against them"*[867]. Where an area of a given city is more monitored than another part of the same city, more incidents may be observed in the places under monitoring than in other areas. More generally, Guillaume Gormand shows that the monitoring of certain places implies the application of certain filters in terms of people to be followed or of particular actions to be scrutinised. The creation of these filters is not based on *"formal and specific rules"*, but on a set of parameters that are highly subjective and linked to the experience, training, views and missions of the operator. As a result, these filters may lead to *"a significant degree of injustice"*.[868]

Another example of human weakness is given by the same author[869]. He reports that in a video-surveillance system it is not uncommon for officers in charge of surveillance to be tempted to point the camera at women, based on their physical appearance. In addition to constituting a diversion of the system's purposes, this constitutes a gender-based discrimination, due to a personal tendency of operators to discriminate between genders.

Finally, it might be argued that the choice of biometry – and, further, video-surveillance – in order to fulfil a purpose of security is, in itself, a

human-based course error. Indeed, as highlighted by Agamben, biometric identification does not bring any security[870]: it only enables – eventually[871] – the identification of persistent offenders and persons who are already known for being in the course of preparing an offence. It is the reason why biometric surveillance, as well as video-surveillance, appears to be disproportionate. Indeed, both result in the monitoring of a majority of persons who are absolutely innocent and should not be under scrutiny.

Worse, it appears that a reasonable number of persons whose photographs are stored in some databases used to compare results from video-surveillance have not been convicted of any offence, which means that they are perfectly innocent. It is the case with the United Kingdom biometric database. Even though a court decision has ruled that such photographs should be deleted, the Home Office explained that it would be *"extremely lengthy and resource intensive"* to do so, because *"the police national database does not link custody images to individual crime records"*.[872] Moreover, the UK Commissionner for the retention and use of biometric material observed that the *"somewhat anarchic situation"*, in terms of facial images governance and standards, *"runs the risk of false intelligence or wrongful allegations"*[873]. Incidentally, this situation shows that, despite the fact that there is no evidence of the technology's efficiency to fight criminality, some governments prefer to invest in technological developments rather than in the safeguarding of citizens' basic rights.

It might be the reason why biometric and behavioural research focusses on prediction and anticipation, in an ideal of anticipating crime before it is committed[874]. 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. Indeed, the prediction of behaviour 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.[875]

3) RISKS OF THEFT OF BIOMETRIC IDENTIFIERS

Biometric data may be vulnerable to risks at four levels, which are presented below. They correspond to four possible attack strategies.

• At the data subject level

In standard authentication systems, basic rules of security such as a password make it possible to reasonably prevent the extraction of sensible information. The use of tools such as a password wallet[876] or a cloaked password[877] can deceive or postpone even coercive action against the holder of the information.

In biometric authentication systems, original biometric identifiers cannot be hidden. Consequently, the standard theft of personal items may be sufficient to reconstruct biometric data without the knowledge of the person concerned. For example, the theft of a glass or of a high-resolution photograph may enable access to fingerprints[878] and characteristics of the face and iris. 879 In extreme cases, coercive measures may enable attackers to obtain the biometric identifier (such as fingers for fingerprints), with no possibility, for the victim, to mislead them.

• At three other levels that might be located either on the side of the person to be identified, or remotely.

o The device that captures the biometric data to be compared to the database (example of a fingerprint reader).

o The technology that assesses whether a match exists between the original data and the data included in the database (this technology is in the system that contains the biometric identifiers database).

o During the transit between the capture and the matching phases (which is usually the network used to carry the data).

In standard authentication systems, if basic rules of security are implemented, the impact of a theft, at the three above-mentioned points of attack, is generally quite reduced whereas the impact of the theft of a biometric identifier is, in contrast, of a very high nature.

Indeed, in classical authentication systems, identifiers such as passwords are generally protected with a cryptographic technique, which turns the original identifiers into a degraded version of it, called a *"hash"*. The use of a hash makes it possible to recognise a match between the hash and the original identifier, but not to recreate the latter. Each *"hashing"* procedure applied on the same identifier will provide for a different hash. As a result, a theft of a hash has limited incidence, because the hash can only be reused on the service that produced the hash. This hash will not be reusable on other services.

Further, even if not hashed, the theft of an identifier might have the same limited incidence if the security rule that requires different passwords for different services is followed.

In biometric authentication systems, the biometric identifier cannot be hashed. It is only transformed into a *"feature vector"*, which is a reduced version of it. This reduced version does not enable, as such, the recreation of the original biometric identifier (for exemple a face or a fingerprint). However, for a same biometric identifier, the feature vector will be the same each time the same encoding technique is used to create it. In case different encoding techniques are used by several providers, a feature vector obtained with one of them is commutable into a feature vector obtained with another encoding technique. Consequently, any interception of feature vector can lead to data reuse on multiple services, in the pursuit of numerous purposes, without the person concerned being aware of it.

In addition, in classical systems, a theft of a password can be easily countered by a modification of this password, on the service concerned. In case the password is used for several services, the modification must only be spread to these very services. In biometric authentication systems, the original biometric identifiers (such as a face image or a fingerprint) will be usable, by design, on every other biometric based system. However, this identifier cannot be changed[880]. Even if a modification was possible, it would not be sufficient to bring it in the compromised system. The modification would have to be spread in all existing systems that use the same identifier.

4) IMPACTS IN TERMS OF REVERSAL OF THE BURDEN OF PROOF

Technology-based and human-based errors are worrying in relation to biometric identifiers, because these identifiers are presented as *"the most reliable ways of perfecting [...] trust"*[881].

Indeed, a lack of identification, for example at an airport when crossing borders, may lead to a deprivation of the freedom of movement. The identification of persons by mistake may lead to unjustified deprivation of liberty or to discrimination[882], depending on the aim that is pursued. In the United Kingdom, it is already reported that *"there are lots of people who have been wrongly stopped by the police and – in some cases – had some quite traumatic incidences as a result"*.[883]

A lack of identification might also result in a violation of the right to a fair trial if the use of biometry leads to a reversal of the burden of proof.

In all these situations, the victim of a mis-identification may have to demonstrate this mistake. However, under the ECHR legal system, the burden of demonstrating the necessity and the proportionality of a restriction of freedom is borne by the person or the entity that decides to bring this restriction. This reversal of the burden of proof therefore impacts several rights, mentioned above, in violation of the ECHR.

Finally, it is worth noticing that this reversal of the burden of proof also represents an unlawful fusion between authentication and accountability. In the present case, the reason is that a mistaken identification leads to attributing to the wrong person a particular treatment afforded to someone else. There are several other examples of attribution of liability, to a person, based on his or her identification, whereas there is no formal link between identity and accountability. The most powerful example of this is the IP address, which may identify the holder of an Internet account

[884]. There were several temptations to consider the holder of an IP address as being the potential author of a penal offence committed on the Internet[885], despite the unreliability of this identifier[886]. Temptations of the same kind are even more to be feared in relation to biometric identifiers, which are widely reported as trustworthy.[887]

5) IMPACTS ON THE RIGHT TO A FAIR TRIAL AND ON HUMAN DIGNITY

Negation of the presumption of innocence

The mass monitoring of publicly accessible places leads, according to Yves Poullet, to the stigmatisation *"any individual as a suspect, by default"*[888]. This is directly contrary to the presumption of innocence[889]. Further, the author 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.

Negation of the principle that offences and penalties must be defined by law

As a result of this general stigmatisation, and because the factors that are monitored are generally not known[890], individuals may commit a *"fault"* without being aware, in advance, that their particular behaviour or action constitutes a fault. This is absolutely contrary to the principle that offences and penalties must be defined by law, in order to ensure foreseeability. This principle is one of the last ramparts against arbitrariness.

Impacts on dignity

In addition, the collection of a biometric identifier induces the possibility that a large number of persons will access this identifier, thus depriving the individual of the possibility to choose who will access this intimate data and how this identifier will be used. This takes place in a context where any single undue access might have terrible consequences, because the identifier cannot be revoked. Before the United Kingdom House of Commons Science and Technology Committee, Professor Martyn Thomas explained in 2005 that *"the theft of an individual's biometrics [creates] a "*security nightmare*" whereby somebody's biometrics [are] 'no longer available to them to authenticate themselves for the rest of their lives'"*[891]. Despite this concern, practices show that more than 15 years afterwards, this kind of security is not the priority of several governments and institutions.

Access might firstly be due to a security issue. We have already analysed that the security of biometric identification systems is relative. In addition, at national levels, some states used biometric identification systems to grant a wide number of services with a power to access databases for internal security purposes, which multiplies risks in terms of undue access and security issues.[892] This takes place in a context where, at the level of certain states, the management of databases containing citizens' personal information can already be criticised.[893]

This situation leads to a quasi-absolute deprivation of the right, for a person, to consent to the use of his or her biometric information. This appears to be an intolerable threat to human dignity.[894]

6) IMPACTS ON THE CREDIBILITY OF THE FIGHT AGAINST TERRORISM

The use of biometric identifiers for the purposes of security, and more precisely to fight terrorism and manage borders, constitutes in itself a wish to discriminate people based on their physical and biological characteristics. At first glance, the discrimination concerns people who do not benefit from certain rights, compared to persons who benefit from these same rights, based on their authentication. Examples of rights concerned are the crossing of a border or the possibility to stay in a publicly accessible place without being arrested.

However, any use of biometry to predict behaviours, based on physical and behavioural factors, results in the discrimination of persons based on their nature, character, appearance, social origin, or ethnicity. Such discrimination is prohibited by the ECHR[895].

This is perfectly illustrated by Ayse Ceyhan, who highlights that the EU *"still mixes security control logic [...] with utilitarian logic consisting in welcoming qualified migrants"*. The main feature of this mechanism is its *"proactive and predictive function"*. [...] Indeed, it does not only aim to manage migration flows, but also to detect 'individuals at risk' before their entry into the European territory".[896]

Moreover, a NGO puts forward that the detection of persons *"at risk"* is mainly based on ethic characteristics at the European level. It states that the *"EU justice and home affairs ministers"*,

in response to terrorist attacks that took place in France and Austria, singled out *"migrants (explicitly) and Muslims (implicitly) as a problem"*, even though they asserted a need *«to combat all forms of violence which target people on the basis of their actual or supposed ethnic origin, or their religious belief or on the basis of other types of prejudice"*.[897]

The use of criteria such as *"homeless"* or *"foreign appearance"*, within the framework of video-surveillance, was also demonstrated by other authors[898].

There is therefore an explicit contradiction, a *"damning paradox"*[899] to combat terrorism in the name of values that include the right to non-discrimination, using discrimination based on ethnic and social characteristics. This contradiction, in addition to constituting a violation of the ECHR, undermines the credibility of the fight against terrorism in the name of European values.

Similarly, Fran ois Sureau, lawyer at the French Council of State and Court of Cassation and a Member of the Acad mie Fran aise, argues that the high restrictions brought to citizens' fundamental rights in the name of the fight against terrorism *"does not add anything"* to this fight. On the opposite, he believes that this affords terrorism:

"a victory without a struggle, because it shows how weak our principles were".[900]

5.3.5 RISK FOR DEMOCRACY

1) A POSSIBILITY OF ABUSE THAT WAS NEVER REACHED IN HISTORY

We analysed that the processing of biometric data, by a third party including a state, represents a genuine, current, and serious threat to the right to self-determination and to human dignity.[901] Both these rights suffer no limitation in a democracy governed by the rule of law, since they constitute the core of fundamental rights.[902] In other words, they constitute a zone that cannot be crossed, the *"limit to the limits"* that *"should be respected under any circumstances, [because] its infringement should be unjustifiable"*[903].

Consequently, the processing of biometric identifiers of a whole national population, and, worse, of the whole European population in addition to people from other countries based on the EU migration policy, as well as, without doubt, data exchanges with other regions of the world[904], appears per se impossible to justify as part of an approach that aspires to be proportionate to its purpose, if this purpose is not a purpose of social control.

Such a systematic biometric identification appears far more difficult to justify than the one resulting from the creation of a unique non-biometric national ID, which had however previously stirred up strong emotions at the time of its creation in France[905].

The use of biometric identifiers together with technologies that enable biometric recognition or identification, particularly at a large scale in public places, further raises the level of interference with freedoms. The possibility of abusive use and of abusive interconnections, which are already noticed in relation to non-biometric technology and files at government levels[906], before any beginning of execution of a prohibited action and without any possibility of revocation, are indeed at their maximal level, a level that was actually never reached in human history.

2) THE CIRCUMVENTION OF DEMOCRATIC CHECKS AND BALANCES

Facing this situation, any political democracy concerned about human rights would have either stopped the use of such technology, or – at the minimum - created the conditions for proper societal debate, in order to collect, understand and take into account opposing views. Such debate is especially commanded by the Council of Europe Convention on Human Rights and Biomedicine[907], which clarifies that human dignity must prevail *«over the sole interest of society or science"*.[908] European countries have moreover committed themselves to respect human dignity[909].

Instead, 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.[910] For at least two decades, we have been experiencing disproportionate restrictions to freedoms that are claimed to be justified by a need

for security, which is presented as conditional to the exercise of other freedoms, thus operating a reversal of value.[911] At the same time, *"few multidisciplinary official studies have been made public regarding the pros and cons on biometric surveillance systems"*[912], as if the impacts of these systems *"were secondary"*[913].

Even though some parliamentary members still criticise this approach, one of them having for example termed it a *"negation of the key principles of democracy"*[914], public representatives and legal instruments concomitantly resort to assertions that tend to discredit the legitimacy of people who call for a return to the application of the rule of necessity and proportionality. As we analyse it, this form of communication contributes inter alia to weaken parliamentary opposition by discouraging contrary opinions. This takes place in a context where the powers of the parliament might be already undermined by several mechanisms. Such a situation sends out a clear signal that concerned governments disregard counter-powers, which may in turn prompt parliamentarians to adopt proposed laws in order to avoid being deprived of the possibility to discuss further acts.[915] In this regard, Fran ois Sureau evokes a *"pre-totalitarian"* situation[916], specifying that each time a law is contrary to the philosophy of preservation of freedoms, this very philosophy is lost a bit more as a value[917].[918]

3) A CLEAR SIGNAL OF UNACCEPTABLE PATERNALISTIC DECISION-MAKING APPROACH

This context as a whole constitutes itself a clear signal that the European Union and States are tempted by social control. We already analysed that such a temptation is inherent to any State[919]. In addition, the mere existence of technology may represent an easy way to follow such a path. Edgar A. Whitley and Gus Hosein observe that *"it is no longer the case that technology simply supports the implementation of policy decisions; instead, technology can now be a key driver of innovative practices"*[920].

The notion of social control may cover different situations. It may firstly refer to a conception exposed in the *"Surveillance Studies"*[921], in which the government seeks to assert control over citizens, through a surveillance which produces *"a knowledge that can build up of individuals, groups [and] legal entities"*, and which necessarily entails the urge to guide, modify, correct or normalise behaviours, due to the feeling of citizens to be monitored and to the knowledge gained on them.[922]

Social control may more simply refer to a *"paternalistic 'best interests' decision-making"* that would *"overrid[e] or ignor[e]"* the *"will and preference of persons"* who are in a position to give their opinion.[923] Practical examples of such paternalistic approach have been reported, including by Edward Snowden[924], a French professor of Management Science[925], and law enforcement representatives in France[926] and in the United Kingdom[927].

In any case, social control is not acceptable, and paternalistic *"best interests' decision-making"*[928] is not a democratic political path. Public institution representatives have no legitimacy to consider themselves as better advised than citizens to make choices that modify the nature of the political regime. On the contrary, the ECtHR recalled that *"any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard"*[929]. Through the EUCFR, such assertion is applicable to the institutions of the European Union.

4) THE RISK OF DISAPPEARANCE OF THE RIGHT TO RESIST OPPRESSION

One of the most obvious impacts this situation generates is *"the collapse, in the future, of any possibility of effective exercise of the fundamental right to resist oppression, corollary to individual freedom itself*[930]*"*. This was highlighted by one hundred and twenty members of the French Parliament in the context of an attempt by the state to create, in 2012, a biometric identity card, which was qualified as *"the file of honest people"*[931]. Despite this opposition, the database was established in 2016, by means of a decree.

The preservation of the practical possibility to resist oppression is of utmost importance. This preservation makes it possible to choose liberal democracy as a political system[932], *"not only from Law, which, instead of guaranteeing rights and protecting freedoms, manifestly breaches them, but also from the system which enables that such laws might be issued"*[933].

To illustrate this crucial need, we can cite Raymond Forni, once Vice-President of the French Data Protection Authority and President of the French National Assembly[934]:

"In a democracy, I think that it is necessary that there exists a room for fraud. If false identity cards could not have been manufactured during the war, tens of thousands of men and women would have been arrested, deported, undoubtedly dead. [Without such a room] there is no real democracy".

Disappearance of the practical possibility to exercise the right to resist oppression is not acceptable in a democracy governed by the rule of law. In essence, such disappearance would mean that liberal democracy itself has already disappeared. It would mean that the core of fundamental rights, including the right to dignity and to self-determination[935], themselves disappeared – based on the denial of the democratic constitutive elements that are the requirements for necessity and proportionality of any limitation of right[936].

Actually, the possibility for States to, systematically, uniquely identify any individual, within the framework of a travel or of the search for the perpetrator of an offence, as well as in a multitude of alternative purposes, already constitutes a great threat to the right to resist oppression. Together with the possibility to remotely identify individuals in publicly accessible places, in real time or after recording, it leads, in practice, to the suppression of the very possibility to resist. This has been perfectly shown by a law enforcement representative, who explains the following:

"The benefit of [facial recognition] is to systematically and automatically execute the law enforcement basic acts which are identification, monitoring and search for individuals, while rendering such control invisible. Under the reserve that algorithms are free of bias, it could end recurrent polemic relating to ethnic profiling, since identity checks would be persistent and general. At the same time, it would enable greater responsiveness in relation to the search for vulnerable persons or to the tracking of fugitive offenders. It would also be likely to result in a self-monitoring which would reduce incivilities […] in the same way as the social credit Chinese model"[937].

5) THE NEED TO SETTLE THE PROPER CONDITIONS FOR UNDERSTANDING AND DEBATING DEMOCRACY AND PRESERVATION OF FREEDOMS

Consequently, citizens must be placed in a position to make a collective choice in relation to the values that society must protect, and in relation to the means to be used in order to enforce such values. States have the duty to ensure that the best contextual parameters are set up in order to enable such opinion to be issued, through the organisation of an effective public debate where necessary.[938] This obligation notably requires disseminating the culture of democracy, human rights and the rule of law, with a view to enabling citizens to understand what is at stake and to make an informed choice[939], and to enable public and political representatives to make accurate statements.

6) THE NEED TO PUT AN END TO THE MISREPRESENTATION OF REALITY

Indeed, previous analyses show that in a democracy governed by the rule of law, the requirement for security must be considered as an objective that may justify some restrictions of fundamental freedoms. In other words, security is an exception to freedom, to be organised under the strict conditions established in the ECHR.[940]

One of the first conditions for informed, free and frank debate would be to stop contrary assertions, which deny the legal instruments that base human rights preservation. In this respect, Friedrich A. Hayek highlights that *"nothing is more fatal than the present fashion of intellectual leaders of extolling security at the expense of freedom"*[941], because it makes citizens lose sight of the very meaning of freedom. In the same line, the legal instruments restricting freedoms should present things as they are, without hiding them under the guise of a reinforcement of peoples' rights. This is the price for democracy. Human self-determination and dignity cannot be an object of political and marketing[942] games.

Stakes are all the more serious and preoccupying that they seem to be the outcomes of an intention to avoid them – provided the latter is not an excuse[943].

François Sureau showed it before the French Constitutional Council through this articulated statement:

*"After the Bataclan attacks, the husband of a victim published a letter in which he stated […]: 'You will not have my hatred'. The law maker, for its part, seems to publish at the occasion of each new law an open letter to Daesh in which it declares "*You will not have our hatred; but look, you can have our freedoms".[944]

Indeed, the lawyer noticed that where the lawmaker gives overly vague powers to prevention and law enforcement services, these powers are actually *"practically totalitarian"*. He considers *"paradoxical that such kind of texts be regarded as enabling a victory against Islamic terrorism, whereas it represents the opposite: an abdication, an absolute subjugation, even more striking because of its very excess, to the mindsets of our morals adversaries"*[945].

In such a context, there is a clear need to conduct an effective assessment of the proper democratic functioning of the European Institutions and of the EU member states, and to draw conclusions relating to what must be implemented in order to correct dysfunctions.

Indeed, comprehensive and rigorous analysis of the compliance with fundamental rights of each biometric identification and recognition technology and practice, and the adoption of a corresponding appropriate legislation to base and frame it, can only be ensured in states where democratic checks and balances are effective. These checks and balance include parliaments, courts and independent authorities.

Pending the results of this evaluation, an immediate moratorium should be declared in relation to technologies and practices that are likely to impact self-determination and human dignity. These technologies and practices could be determined through the evaluation of a certain number of criteria such as: (1) the proximity of the data storage to the person concerned and the number of persons who can access it; (2) the accuracy of the biometric identifier; and (3) the existing possibilities to reuse it in other purposes.

Technologies and practices to be prohibited must include the indiscriminate collection by states and by the industry of biometric identifiers of citizens and residents. They must also include real time and post identification in publicly accessible places, such as some states already did in a more or less achieved manner[946]. They must also include biometric and behavioural recognition and classification, performed without the consent of the people concerned. In addition, these technologies must not lead taking decisions against the persons involved or any other human being without the explicit and informed consent of the people concerned.

706. See subsection 4.1.2.2 of the current study, especially the court case ECtHR, 5th Sect., 17 December 2009, Gardel v. France, appl. n° 16428/05, §58, http://hudoc.echr.coe.int/eng?i=001-96457.

707. See subsection 2.3 of the current study.

708. See subsection 4.1.2.5 of the current study.

709. See subsection 4.1.2.10 of the current study.

710. See subsection 4.1.3 of the current study.

711. ECtHR, gr. ch., 16 February 2000, Amann v. Switzerland, appl. 27798/95, § 70, http://hudoc.echr.coe.int/eng?i=001-58497; CJEU, 20 May 2003, Österreichischer Rundfunk and Others, joined cases C-465/00, C-138/01 and C-139/01, § 75, https://curia.europa.eu/juris/liste.jsf?num=C-465/00&language=en; CJEU, 8 April 2014, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, § 33, http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12.

712. Antoinette Rouvroy and Yves Poullet, 'The right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in Serge Gutwirth et al., Reinventing Data Protection?, January 2009, p. 45-76, https://www.researchgate.net/publication/225248944_The_Right_to_Informational_Self-Determination_and_the_Value_of_Self-Development_Reassessing_the_Importance_of_Privacy_for_Democracy, p. 13. Authors refer partly to Paul De Hert and Serge Gurtwirth ('Privacy, Data Protection and law enforcement. Opacity of the Individual and Transparency of Power'', in Eric CLAES, Antony Duff, Serge GUTWIRTH (eds), Privacy and the Criminal Law, Antwerpen-Oxford: Interscientia, 2006, p. 64). See subsections 4.1.2.11 and 4.1.1 of the current study.

713. See subsection 4.1.2.1 of the current study.

714. Article 32 of the GDPR requires the implementation of "appropriate technical and organisational measures to ensure a level of security appropriate to the risk", taking into account, inter alia, "the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". Ensuring a level of security appropriate to the risk, determined in terms of likelihood and severity, is the very purpose of a risk analysis – and cannot be done without performing a risk analysis.

715. On the risk assessment methodology, see for example the EBIOS method for assessing and treating digital risks, https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/.

716. The detailed presentation of this requirement can be found in subsection 4.1.3.1 of the current study.

717. Example of the city of Montpellier, which does not even mention the administrative act that authorises the implementation of video-surveillance: https://www.montpellier.fr/3453-le-csu.htm.

718. See for example Préfecture de la Somme, Arrêté portant autorisation provisoire d'un système de vidéoprotection : ville d'Amiens 80000, 24 June 2020, in Recueil des actes administratifs, spécial, n° 2020-059 of 26 June 2020, p. 22, https://www.somme.gouv.fr/content/download/32695/201402/file/recueil-2020-059-recueil-des-actes-administratifs-special.pdf. This document only refers to purposes that are authorised by the legislation (Internal Security Code, articles 223-1 s. and 251-1 s.) such as the prevention of terrorism or assistance to persons (article L. 251-2). This is nonsense, since proportionality can only be assessed in the light of the actual specific purposes that are pursued.

719. Home office, Surveillance Camera Code of Practice, June 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

720. N° 3.1.1 of the Code of Practice. See also n° 3.2.3 in relation to facial recognition.

721. N° 3.2.3 and 3.2.4 of the Code of Practice.

722. Tony Porter, Survey of Local Authorities Compliance with the Protection of Freedoms Act 2012, 20 October 2020, https://videosurveillance.blog.gov.uk/2020/10/20/survey-of-local-authorities-compliance-with-the-protection-of-freedoms-act-2012/. See subsection 7.2.2 of the current study.

723. N° 3.2.3 and 3.2.4 of the Code of Practice.

724. See subsection 4.1.3.4.1. of the current study.

725. See, in particular, subsections 3.3 and 4.1.5 of the current study.

726. Decree n° 2016-1460 of 28 October 2016 autorising the creation of a personal data processing relating to passports and national identity cards, article 1, as modified by decree https://www.legifrance.gouv.fr/loda/id/LEGIARTI000033326510/2016-10-31/.

727. Article 4 of the decree n° 2016-1460 of 28 October 2016, already mentioned. See also Article L122-1 of the Internal Security Code, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042919869/.

728. See subsection 4.1.3.1 of the current study.

729. See for example Council of Europe, 'Mass surveillance: who is watching the watchers?', April 2016, ISBN 978-92-871-8104-6, n° 18, 47, 50 and 53 s. See also Kurt Zindulka, 'Definitely Not Authoritarian: Britain to Introduce Facial Recognition App for Government Services', 14 October 2021, Breitbart, https://www.breitbart.com/europe/2021/10/14/definitely-not-authoritarian-uk-to-use-facial-recognition-for-govt-services/. The Author refers to a testimony from the director of the civil liberties campaign group Big Brother Watch, Silke Carlo, before the Committee on Justice and Home Affairs in the House of Lords: "Concerns have also been raised that the use of facial recognition could be used to monitor and potentially clamp down on protest movements. Indeed, Breitbart London reported in February that police forces throughout the country have already been using drones to monitor and track protests, including those against the authoritarian lockdowns imposed by the government".

730. See subsection 3.3 of the current study. The call for a ban on facial recognition in public spaces

is itself recognised in the Impact assessment that accompanies the proposed artificial intelligence act: Commission staff working document impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, SWD/2021/84 final, n° 2.1.2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084.

731. See subsection 5.1.5 of the current study.

732. On this question, see subsection 3.1.1 of the current study.

733. Estelle De Marco, 'La captation des données', in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux, Institut Universitaire Varenne, coll. colloques et essais, 4th trim. 2017, p. 91-107 [p. 104].

734. See for example article 40 of the French penal procedure Code.

735. See subsection 4.1.2 of the current study.

736. See subsection 4.1.3.1 of the current study.

737. See subsections 4.1.2.1 and 4.1.2.11 of the current study.

738. See subsection 4.1.3.2 of the current study.

739. Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, SWD/2018/110 final - 2018/0104 (COD), respectively subsections 2.1.1 and 1.2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52018SC0110. The eIDAS Regulation (Regulation on electronic Identification and Authentication Services), entered into force in 2016, is the object of a proposal for modification: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=SWD:2021:124:FIN.

740. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), n° 3.17 - 3.19, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.

741. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 3-8; David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 15.

742. See the list of the systems on the eu-LISA website (https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems) and the EU page related to "Smart borders systems" (https://ec.europa.eu/home-affairs/pages/glossary/smart-borders-package_en).

743. Article 29 Data Protection Working Party, opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism", adopted on 9 November 2004, WP99, n° 5.8 and 5.12, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf

744. Decree n° 2016-1460 of 28 October 2016 authorising the creation of a personal data processing relating to passports and national identity cards, article 1, as modified by the decree https://www.legifrance.gouv.fr/loda/id/LEGIARTI000033326510/2016-10-31/.

745. See subsection 4.1.3.2 of the current study.

746. Article 29 Data Protection Working Party, opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism", adopted on 9 November 2004, WP99, p. 4, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp99_en.pdf.

747. See subsection 4.2 of the current study.

748. See for example David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 109; Paul Bischoff, Surveillance camera statistics: which cities have the most CCTV cameras?, 17 May 2021, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/: "As you can see from the above chart, a higher number of cameras just barely correlates with a lower crime index"; Laurent Mucchielli, 'Vidéosurveillance : que voient les opérateurs derrière les caméras ?', 2 October 2011, in Vous avez dit sécurité ?, ed. Champ Social, coll. Questions de société, 2012, p. 157-162, https://www.cairn.info/vous-avez-dit-securite--9782353712397-page-157.htm?contenu=resume; Owen Bowcott, 'CCTV boom has failed to slash crime, say police', 6 May 2008, The Guardian, https://www.theguardian.com/uk/2008/may/06/ukcrime1.

749. . Kurt Zindulka, 'Definitely Not Authoritarian: Britain to Introduce Facial Recognition App for Government Services', 14 October 2021, Breitbart, https://www.breitbart.com/europe/2021/10/14/definitely-not-authoritarian-uk-to-use-facial-recognition-for-govt-services/: "The government has also been seeking to expand the use of facial recognition software in public to assist police in tracking alleged criminals, yet so far the systems have shown minimal ability in actually leading to arrests, with just two people being arrested in trials in London in which over 25,000 people had their faces scanned by police cameras".

750. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 248, https://hal.archives-ouvertes.fr/tel-02439529.

751. In this regard, Edgar A. Whitley and Gus Hosein highlight that "an identity policy that actively encourages individuals to present their date of birth without restriction becomes a political issue, particularly if citizens are compelled to have identity cards": Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 5.

752. Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity

and proportionality concepts and data protection within the law enforcement sector (WP 211), already mentioned, 3.20, referring to ECtHR court cases.

753. ECtHR, 4th Sect., 12 January 2016, Szabó and Vissy v. Hungary, appl. no37138/14, §73, http://hudoc.echr.coe.int/eng?i=001-160020.

754. See subsection 5.3.4 of the current study.

755. Biometric identifiers can be generated in a way that they do not enable a unique world-wide match, but only a decent probability that the holder is the one to be identified within a larger group of people. Such voluntarily «fuzzy» identification might be relatively secure in terms of identification, while it enables, at the same time, a more plausible deniability and the prevention of most misuses. In the same lime, behavioural recognition could be recognised as imperfect to identify thoughts and personality, and consequently not be used to apply decisions to individuals.

756. Research is conducted in relation to people classification and to prevention based on behavioural criteria, which appears extremely intrusive in a number of respects, in particular where biometric databases are available. This issue is recognised in the impact assessment that accompanies the proposal for a regulation. See Commission staff working document impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, SWD/2021/84 final, n° 2.1.3-2.1.4, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084

757. See subsection 5.3.4.3 of the current study.

758. See respectively subsections 4.1.2.2, 4.1.2.1 and 4.1.2.11 of the current study.

759. See subsection 4.1.2.8 of the current study.

760. See subsection 4.1.2.10 of the current study.

761. See subsections 4.1.2.12, 4.1.2.5 and 4.1.2.6 of the current study.

762. In this regard, see subsection 4.1.3.3 of the current study.

763. See respectively subsections 4.1.2.2, 4.1.2.1 and 4.1.2.11 of the current study.

764. See subsection 4.1.3.4.1 of the current study.

765. EDPS opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents, 10 August 2018, p. 3, https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf.

766. They include "faces, […] gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals" and ask for their ban "in any context": EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 2-3, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

767. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 2-3, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

768. They include "faces, […] gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals" and ask for their ban "in any context": EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 2-3, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

769. Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, COM/2018/212 final - 2018/0104 (COD), n° 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0212

770. Consolidated version of the treaty on the functioning of the European Union, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF.

771. For further analysis, see annex 10.1 of the current study.

772. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final, n° 2.1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

773. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 2 and n° 11 p. 7, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

774. For further analysis, see the annex 10.2 of the current study.

775. Decree n° 2016-1460 of 28 October 2016 authorising the creation of a personal data processing relating to passports and national identity cards, article 1, as modified by the decree https://www.legifrance.gouv.fr/loda/id/LEGIARTI000033326510/2016-10-31/.

776. François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 46. See also the preamble of the ECHR.

777. François Sureau, 'Le refus de sacrifier la liberté', Interview from Fabien Escalona and Ellen Salvi for Mediapart, 10 October 19, https://www.april.org/le-refus-de-sacrifier-la-liberte-francois-sureau (transcript) and https://www.youtube.com/watch?v=yYY-B0jZMD4&t=7s (video).

778. François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, Tallandier Essais, 2019, p. 43. See also subsection 7.1.1.3 of the current study.

779. See subsection 4.2.2 of the current study.

780. François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, already

mentioned, p.43 and footnote 24.

781. EDPS opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents, 10 August 2018, p. 3, https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf.

782. EDPS opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents, already mentioned, p. 3-4.

783. Opinion of the European Data Protection Supervisor on the Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (.../...) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), (2011/C 101/03), 15 December 2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:101:0014:0019:EN:PDF.

784. French Constitutional Council, Press Release, 'Décision n° 2012-652 DC du 22 mars 2012 - Communiqué de presse', 22 March 2012, https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2012-652-dc-du-22-mars-2012-communique-de-presse.

785. See subsection 3.3 of the current study.

786. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), already mentioned, p°2.

787. See for example a question from Moritz Körner who asked, on 22 January 2020, the EC opinion on the compatibility with the EUCFR and more generally EU law of practices such as one intended by the German minister of interior, who was planning to "install systems at 135 railway stations and 14 airports in Germany which will enable any individual at those locations at any time to be suspected of committing a criminal offence with no justification and will enable all such people to be individually scanned and assigned personal markers and the markers to be compared with the data of criminals in existing police databases." (https://www.europarl.europa.eu/doceo/document/E-9-2020-000338_EN.html). The EC answered that "the application of the data protection legislation falls primarily under the competence of national authorities, in particular data protection authorities and courts" without drawing appropriate conclusions from this question in the proposal for a regulation (https://www.europarl.europa.eu/doceo/document/E-9-2020-000338-ASW_EN.html).

788. European Parliament, 'Artificial Intelligence in policing: safeguards needed against mass surveillance', Press release, 29 June 2021, https://www.europarl.europa.eu/news/en/press-room/20210624IPR06917/artificial-intelligence-in-policing-safeguards-needed-against-mass-surveillance.

789. François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 6 and 31. See subsection 4.1.1.4.1.3 of the current study.

790. François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 6; Jacques Robert and Jean Duffar, Droits de l'homme et libertés fondamentales, Montchrestien, Lextenso éditions, 8° ed., 2009, p. 2; Olivier Tesquet, Etat d'urgence technologique, Premier Parallèle, 2021, p. 11-12; David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p.5. See also Laurent Laniel et Pierre Piazza, 'Une carte nationale d'identité biométrique pour les Britanniques : l'antiterrorisme au cœur des discours de justification', in Cultures & Conflits, n°64, Hiver 2006, p.49-63, https://doi.org/10.4000/conflits.2174. The authors highlight the «increase of an official rethoric, poorly developed», since the 1980's.

791. See subsection 3.2 of the current study.

792. Olivier Tesquet, Etat d'urgence technologique, Premier Parallèle, 2021p.11; François Sureau in François Sureau dénonce la disparition de l'Etat de droit, dans l'indifférence, https://www.youtube.com/watch?v=F3JCcVi_Gw8. This video was extracted from a video interview of the author in La Grande table Idées d'Olivia Gesbert, 30 September 2019, available at https://www.youtube.com/watch?v=VUgOAr4zPV4.

793. See subsection 4.2.1 of the current study.

794. Such as "If you've got nothing to hide, you shouldn't worry about government surveillance": Daniel J. Solove, Nothing to Hide, The False Tradeoff between Privacy and Security, Yale University Press, 2011, p.1; or "[we accept that] Web giants have a certain number of our data [...] but we don't want to entrust our data [...] to protect ourselves and the other": statement from René-Paul Savary, Senator, on the occasion of the presentation, by the senatorial delegation for strategic foresight of the French Senate, of a report relating to the health crisis: Public Senate, 'Covid-19 : un rapport du Sénat préconise la collecte de données personnelles pour prévenir les crises sanitaires', 3 June 2021, https://www.publicsenat.fr/article/societe/covid-19-un-rapport-du-senat-preconise-la-collecte-de-donnees-personnelles-pour. During this interview, the Senator, together with Senator Christine Lavarde, also declared that there is a "'French taboo' relating to personal data collection".

795. See also Statewatch, New EU proposals foresee mandatory biometrics in national ID cards, 2 May 2018, https://edri.org/our-work/new-eu-proposals-foresee-mandatory-biometrics-in-national-id-cards/. The publication considers that Regulation 2019/1157 "essentially aims at fingerprinting the majority of EU citizens – which will complement the fingerprinting of non-EU citizens as required by the Visa Information System (VIS), for those who require a visa to enter the bloc, and as foreseen by the Entry/Exit System, which will hold the fingerprints on almost all non-EU nationals exempt from visa requirements".

796. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, SWD/2021/84 final, n° 1.1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

797. Commission staff working document impact assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, SWD/2021/84 final, n° 2.1.1-2.1.4, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084.

798. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, SWD/2021/84 final, n° 3.5, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

799. The ECtHR considers that "where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights, the margin of appreciation will tend to be narrower": Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, Council of Europe/European Court of Human Rights, 31 December 2020, n° 431, https://www.echr.coe.int/documents/guide_art_8_eng.pdf, referring to ECtHR, 27 May 2004, Connors v. the United Kingdom, appl. n° 66746/01, § 82, http://hudoc.echr.coe.int/eng?i=001-61795.

800. See French Constitutional Council, 'Décision n° 2012-652 DC du 22 mars 2012 - Communiqué de presse', Press Release, 22 March 2012, https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2012-652-dc-du-22-mars-2012-communique-de-presse.

801. Sylvia Preuss-Laussinotte, 'Bases de données personnelles et politiques de sécurité : une protection illusoire ?', in Identifier et Surveiller n° 64, Hiver 2006, p. 77-95, https://journals.openedition.org/conflits/2133 (translated from French).

802. In relation to this introduction, see subsection 4.1.3.4.1 of the current study.

803. In France, authorisations to implement video-protection do not provide for many details. Websites of public authorities and institutions do not generally provide for sufficient information either. In addition, whereas video-surveillance must be indicated in places where it is implemented under French law, such information is missing in a large number of cities, such as in Montpellier. In the latter city, Guillaume Gormand shows that, in certain monitored area, only 14% of individuals are aware of the existence of cameras (L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 345, https://hal.archives-ouvertes.fr/tel-02439529). In the UK, the report from the Surveillance Camera Commissioner also shows an opacity of certain practices, which are mainly controlled based on declarations and self-assessment. For further details see subsection 5.2.1 of the current study.

804. A document, first reported by the EUObserver website (Nikolaj Nielsen, UK unlawfully copying data from the EU police system, 28 May 2018, https://euobserver.com/justice/141919) established «major deficiencies in the legal, operational and technical implementation of SIS" in the UK that had not been remedied, despite concerns first raised in 2015», posing «serious and immediate risks to the integrity and security of SIS data". Especially, the US government and US companies are suspected to had access «to UK's illegal copies» of the database: Jennifer Rankin, 'UK accused of 'behaving like cowboys' over EU database copying', 9 January 2020, The Guardian, https://www.theguardian.com/world/2020/jan/09/uk-accused-of-behaving-like-cowboys-over-eu-database-copying. In relation to the SIS, see subsection 3.1.1 of the current study.

805. See for example Jean-Pierre Jouyet, President-in-Office of the Council, Debates of 23 September 2008 before the European Parliament, issue 4 'Combating terrorism - Protection of personal data', https://www.europarl.europa.eu/doceo/document/CRE-6-2008-09-23_EN.html?redirect. The author stated "it is a fact that there is very little, or even no regulation of so-called 'sovereign' files, particularly as regards public security". See also subsections 7.1.2, 7.2.2 and 7.3.2 of the current study.

806. Estelle De Marco, 'La captation des données', in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux, Institut Universitaire Varenne, coll. colloques et essais, 4th trim. 2017, p. 91-107.

807. Council of Europe, 'Mass surveillance: who is watching the watchers?', April 2016, ISBN 978-92-871-8104-6, n°9 p.7, which evokes a "culture of secrecy". See also n° 77 p. 35.

808. See subsection 3.1.2 of the current study.

809. See subsection 5.2.4.2 of the current study.

810. ECtHR, 25 May 2021, gr. ch., Big Brother Watch and others v. The United Kingdom, appl. n° 58170/13, 62322/14, 24960/15, § 361, http://hudoc.echr.coe.int/eng?i=001-210077: The French Constitutional Council considers for its part that the principles of clarity, accessibility and intelligibility of the law impose on the law-maker the obligation to "adopt disposals of sufficient precision and non-equivocal formula in order to prevent subjects of the law from an interpretation that would be in opposition with the Constitution or from the risk of arbitrariness": French Constitutional Court, decision n° 2004-503 of 12 August 2004, § 29, https://www.conseil-constitutionnel.fr/decision/2004/2004503DC.htm.

811. ECtHR, plen., 2 August 1984, Malone v. The United Kingdom, appl. n° 8691/79, § 79, http://hudoc.echr.coe.int/eng?i=001-57533; French Constitutional Council, Decision n° 2004-503 DC of 12 August 2004, already mentioned, § 29.

812. See subsection 5.2.4.2 of the current study.

813. Sylvia Preuss-Laussinotte, 'Bases de données personnelles et politiques de sécurité : une protection illusoire ?', in Identifier et Surveiller n° 64, Hiver 2006, p. 77-95, https://journals.openedition.org/conflits/2133 (translated from French).

814. ECtHR, plen., 6 September 1978, Klass and others v. Germany, appl. n°5029/71, § 49, http://hudoc.echr.coe.int/eng?i=001-57510.

815. Eric Töpfer, 'Urban Video Surveillance in Europe: A Political Choice?', in European Forum for Urban Security, Citizens, Cities and Video Surveillance - Towards a democratic and responsible use of CCTV, June 2010, p. 65-79 [p. 69], https://panoptykon.org/sites/panoptykon.org/files/cctv_publication_en_0.pdf. The author refers to David Lyon ('Globalizing surveillance. Comparative and sociological perspectives', in International Sociology, Vol. 19, n° 2, 2004, p. 135-149 [141-142]).

816. ECHR, 5° Section, 10 January 2019, Khadija Ismayilova v. Azerbaijan, appl. n° 65286/13 and 57270/14, § 139, http://hudoc.echr.coe.int/eng?i=001-188993.

817. Paul De Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement: Opacity of the individual

and transparency of power', in Erik Claes, Antony Duff and Serge Gutwirth, Privacy and the criminal law, Hart Publishing, 2006, p. 61-102, n° 3.2, https://www.researchgate.net/publication/254800085_Privacy_data_protection_and_law_enforcement_Opacity_of_the_individual_and_transparency_of_power.

818. See subsection 4.1.2.1 of the current study.

819. Court of Justice of the European Union, Press Release n° 123/20, Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophones and Others, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf, p. 2. See also subsection 4.2 of the current study.

820. ECtHR, gr. ch., 4 December 2008, S. and Marper v. The United Kingdom, appl. n° 30562/04 and 30566/04, § 84-85, http://hudoc.echr.coe.int/eng?i=001-90051. See subsection 5.2.3 of the current study

821. ECtHR, gr. ch., 4 December 2008, S. and Marper v. The United Kingdom, already mentioned, § 125.

822. ECtHR, gr. ch., 4 December 2015, Roman Zakharov v. Russia, appl. n° 47143/06, § 302-305, http://hudoc.echr.coe.int/eng?i=001-159324. See also the section 5.2.6 of the current study.

823. ECtHR, Guide to the Case-Law of the European Court of Human Rights: Data Protection, updated 30 April 2021, n° 368, https://echr.coe.int/Documents/Guide_Data_protection_ENG.pdf.

824. It is one of the characteristics of the "panopticon" society, described by Michel Foucault based on the works of Jeremy Bentham (see the introduction of the current study). Video-surveillance may be seen as panopticon: see for example Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 35, https://hal.archives-ouvertes.fr/tel-02439529.

825. Yves Poullet, 'La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ?' in LEGICOM 2009/1, p. 47-69 [I, C], https://www.cairn.info/revue-legicom-2009-1-page-47.htm.

826. ECtHR, gr. ch., 16 February 2000, Amann v. Switzerland, appl. 27798/95, § 70, http://hudoc.echr.coe.int/eng?i=001-58497; CJEU, 20 May 2003, Österreichischer Rundfunk and Others, joined cases C-465/00, C-138/01 and C-139/01, § 75, https://curia.europa.eu/juris/liste.jsf?num=C-465/00&language=en; CJEU, 8 April 2014, Digital Rights Ireland and Seitlinger e.a., joint cases C-293/12 and C-594/12, § 33, http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-293/12. See subsection 5.1 of the current study.

827. See subsection 3.3 of the current study.

828. See subsection 4.2 of the current study.

829. Court of Justice of the European Union, Press Release n° 123/20, Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophones and Others, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf, p. 2. See also subsections 4.2 and 5.3.1.1 of the current study.

830. ECtHR, 5th Sect., 2 September 2010, Uzun v. Germany, appl. n° 35623/05, § 52, http://hudoc.echr.coe.int/eng?i=001-100293.

831. Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, August 2021, p. 44, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

832. See also, on a "dividualisation" of individuals, Olivier Aïm, Les théories de la Surveillance – Du panoptique aux Surveillance Studies, ed. Armand Colin, 2020, p. 78 s.

833. See for example the computer engineer Benjamin Bayard, who explains that the creation of files on individuals, and the manipulation of those files and the data they contain, is a form of reification. The manipulation concerns objects, not human beings any more. Consequently, the human-human relationship becomes a human-object relationship. Benjamin Bayard and Marc Rees, Pass sanitaire, géopolitique de la Data, copie privée ?, Thinkerview, 15 June 2021, https://www.youtube.com/watch?v=EOWeewIc2CE.

834. Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, already mentioned, p. 44.

835. In the same line see Christiane Wendehorst and Yannic Duller, already mentioned, p. 44.

836. See subsection 5.2.3. of the current study.

837. See subsection 5.3.4. of the current study, relating to errors and theft.

838. See subsection 5.3.4. of the current study, relating to errors and theft.

839. See subsection 4.1.2.11 of the current study.

840. Translated from French: Yves Poullet, 'La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ?' in LEGICOM 2009/1, p. 47-69 [I, C], https://www.cairn.info/revue-legicom-2009-1-page-47.htm.

841. EDPB, Guidelines 3/2019 on processing of personal data through video devices, 10 July 2019, n° 1, https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf.

842. See especially subsection 5.2.1 of the current study.

843. Council of Europe, Mass surveillance: Who is watching the watchers?, Council of Europe Publishing, April 2016, ISBN 978-92-871-8104-6, p. 42. The Council of Europe refers to a November 2013 report by PEN International on the effects of NSA surveillance.

844. EDPB, Guidelines 3/2019 on processing of personal

data through video devices, already mentioned, p. 7: "systematic automated monitoring of a specific space by optical or audio-visual means […] brings about collection and retention of pictorial or audio-visual information on all persons entering the monitored space that are identifiable on basis of their looks or other specific elements. Identity of these persons may be established on grounds of these details".

845. Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', already mentioned, p. 1-2. The author states that facial recognition would be "likely to result in a self-monitoring which would reduce incivilities […] in the same way as the social credit Chinese model" (translated from French).

846. Antoinette Rouvroy and Yves Poullet, 'The right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in Serge Gutwirth et al., Reinventing Data Protection?, January 2009, p. 45-76 [p. 12], https://www.researchgate.net/publication/225248944_The_Right_to_Informational_Self-Determination_and_the_Value_of_Self-Development_Reassessing_the_Importance_of_Privacy_for_Democracy.

847. ECtHR, plen., 7 December 1976, Handyside v. The United Kingdom, already mentioned, § 49; ECtHR, gr. ch., 22 October 2007, Lindon, Otchakovsky-Laurens and July v. France, § 45, appl. n°21279 and 36448/02, http://hudoc.echr.coe.int/fre?i=001-82846.

848. ECtHR, gr. ch., 22 October 2007, Lindon, Otchakovsky-Laurens and July v. France, already mentioned, § 45.

849. European Parliament Resolution of 21 May 2013 on the EU Charter: standard setting for media freedom across the EU (2011/2246(INI)), B, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0203.

850. ECtHR, 2nd Sect., 14 September 2010, Dink v. Turkey, appl. n° 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, §137, http://hudoc.echr.coe.int/eng?i=001-100384; ECtHR, Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, Council of Europe/European Court of Human Rights, December 2011, p. 5, http://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf.

851. Where this restriction of freedom concerns journalist, it is even worse. The Council of Europe highlights that "when authors, journalists or civil society activists are reluctant to write, speak, or pursue research about certain subjects […] or to communicate with sources or friends abroad for fear that they will endanger such individuals by so doing, not only does this affect their freedom of speech, but also everyone else's freedom of information": Council of Europe, Mass surveillance: Who is watching the watchers?, already mentioned, p. 42.

852. Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, August 2021, p. 8, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf.

853. Christiane Wendehorst and Yannic Duller, already mentioned, p. 21. See also p. 10.

854. See subsection 3.1 of the current study.

855. See subsection 4.1.2.5 of the current study.

856. Bernadette Dorizzi, 'Les taux d'erreur dans le recours aux identifiants biométriques', in Ayse Ceyhan and Pierre Piazza, L'identification biométrique : Champs, acteurs, enjeux et controverses, Editions de la Maison des Sciences de l'Homme, 2011, p. 125-140.

857. Bernadette Dorizzi, already mentioned, p. 129.

858. See subsection 3.2 of the current study.

859. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p.140-141.

860. Christiane Wendehorst and Yannic Duller, already mentioned, n° 3.3.2 p. 51. See also NIST, 'NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software', 19 December 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

861. David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 129.

862. Damien Gayle, 'Met police deploy live facial recognition technology', 11 February 2020, The Guardian, https://www.theguardian.com/uk-news/2020/feb/11/met-police-deploy-live-facial-recognition-technology.

863. Rowland Manthorpe and Alexander J Martin, 81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says, 4 June 2019, Sky News, https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941.

864. Christiane Wendehorst and Yannic Duller, already mentioned, p. 97.

865. Christiane Wendehorst and Yannic Duller, already mentioned, p. 54.

866. David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 150, referring to D. Nelkin and L. Andrews, 'Surveillance creep in the genetic age', in David Lyon (ed.), Surveillance as social sorting: Privacy, risk and digital discrimination, 2003, London and New York: Routledge, p. 95).

867. David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 150, referring to A. Gosline, 'Will DNA profiling fuel prejudice?', in New Scientist, 9 April 2005.

868. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 358, https://hal.archives-ouvertes.fr/tel-02439529.

869. Guillaume Gormand, already mentioned, p. 354.

870. Olivier Aïm, Les théories de la Surveillance – Du panoptique aux Surveillance Studies, ed. Armand Colin, 2020, p. 110, referring to Giorgio Agamben, 'Comment l'obsession sécuritaire fait muter la démocratie', in Le Monde diplomatique, January 2014.

871. Several studies show the very weak impact of video-surveillance and biometric surveillance in

combatting crime. See subsection 5.2.2 of the current study and previously in the current subsection.

872. Alan Travis, 'Police told to delete on request millions of images of innocent people', 24 February 2017, The Guardian, https://www.theguardian.com/uk-news/2017/feb/24/police-told-to-delete-on-request-images-of-innocent-people. See subsection 7.2.1.3 of the current study.

873. Paul Wiles, Commissioner for the retention and use of biometric material, annual report 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644755/CCS207_CCS0917991760-1_Biometrics_Commissioner_ARA_Accessible.pdf. Citations can be respectively found n° 300, 304 and 303.

874. Olivier Aïm, Les théories de la Surveillance – Du panoptique aux Surveillance Studies, ed. Armand Colin, 2020, p. 111. On the research aiming to identify criminals based on their physical and biological characteristics, see Annemarie Sprokkereef and Paul De Hert, 'Ethical practice in the use of biometric identifiers within the EU', January 2007, in Law, Science and Policy, 2007, Vol. 3, pp. 177–201 [177-178], 1475-5335/07 ©2007 A B Academic Publishers, https://www.researchgate.net/publication/228369691_Ethical_practice_in_the_use_of_biometric_identifiers_within_the_EU.

875. In relation to the delivering of targeted advertising based on the analyses of faces and the classification of people by "ethnicity", see for example Matt Burges, 'Europe makes the case to ban biometric surveillance', Wired, 7 July 2021, https://www.wired.co.uk/article/europe-ai-biometrics.

876. The wallet contains passwords that are even not known by the holder of the accounts.

877. A cloaked password is a real password that unlocks a real account, which is a copy of the account to be secured. The provision of the password therefore compromises the copy and not the original account.

878. Kraken Security Labs, 'Bypasses Biometric Security With USD 5 In Materials', 22 November 2021, https://cryptonews.com/videos/kraken-security-labs-bypasses-biometric-security-with-5-in-materials.htm; Hackers also cloned the fingerprint of a Minister based on a photograph and unlocked a smartphone using a fingerprint stolen on a glass of water: Anne Confolant, 'Un hacker clone l'empreinte digitale d'une ministre allemande à partir de photos', 2 January 2015, https://www.itespresso.fr/hacker-clone-empreinte-digitale-ministre-allemande-partir-photos-85769.html. See also Arthur Vera, 'Ces hackers chinois parviennent à déverrouiller un smartphone avec… un verre d'eau', 1 November 2019, https://www.presse-citron.net/ces-hackers-chinois-parviennent-a-deverrouiller-un-smartphone-avec-un-verre-deau/. Scott Sayce, 'Cybersecurity : the future risk of biometric data theft', CNA Hardy https://www.cnahardy.com/news-and-insight/insights/english/cyber-securit-the-future-risk-of-biometric-data-theft. The author states: "Spoofing is the practice of 'fooling' a biometric security system using fake or copied biometric information".

879. Cameron Camp, 'Had your face stolen lately?', 6 October 2020, Welivesecurity, https://www.welivesecurity.com/2020/10/06/had-face-stolen-lately-biometrics-data-breach/. Steve Symanovich, Biometric data breach: Database exposes fingerprints, facial recognition data of 1 million people, Norton, https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html.

880. See especially House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, 25 February 2015, HC° 734, n° 71, https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf: "Unlike a password or PIN code, an individual's biometric characteristic cannot easily be revoked or reissued if it is compromised".

881. David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 125.

882. See subsections 4.1.2.7 and 4.1.2.8 of the current study.

883. . Kurt Zindulka, 'Definitely Not Authoritarian: Britain to Introduce Facial Recognition App for Government Services', 14 October 2021, Breitbart, https://www.breitbart.com/europe/2021/10/14/definitely-not-authoritarian-uk-to-use-facial-recognition-for-govt-services/. The Author reports a statement from the director of the civil liberties campaign group Big Brother Watch, Silke Carlo, before the Committee on Justice and Home Affairs in the House of Lords.

884. An IP address is a number that enables the identification of a computer or a server on the Internet. It is provided by the Internet access provider. It can be static (in this case, it is attributed to a person only) or dynamic (in this case, it is shared by several successive persons). A static IP address, or a dynamic IP address which is correctly time stamped, therefore enables to identify the holder of the Internet account.

885. See for example the discussion relating to the French legislation on the repression of counterfeiting on the Internet: Estelle De Marco, 'Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux', 4 June 2009, http://www.juriscom.net/documents/pi20090604.pdf.

886. An IP address can be compromised. In addition, the holder of an internet account might not be the person who uses the Internet access.

887. This danger is perfectly illustrated by a statement from Lord Steyn's, reported by the representative of the South Wales Police : «It is of paramount importance that the law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science. Such real evidence has the inestimable value of cogency and objectivity. It is in large measure not affected by the subjective defects of other testimony. It enables the guilty to be detected and the innocent to be rapidly eliminated from inquiries»: High Court of Justice, Queen's Bench Division, Divisional Court, Cardiff Civil Justice Centre, [2019] EWHC 2341 (Admin), 4 September 2019, n° 5, https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf.

888. Translated from French: Yves Poullet, 'La loi des données à caractère personnel : un enjeu fondamental pour nos sociétés et nos démocraties ?' in LEGICOM 2009/1, p. 47-69 [I, C], https://www.cairn.info/revue-legicom-2009-1-page-47.htm.

889. François Sureau, Pour la liberté –

Répondre au terrorisme sans perdre la raison, Tallandier Essais, 2019, p. 38-39.

890. *Some LE representative evoke the monitoring of "incivility": Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', Note du CREOGN, n° 43, September 2019, p. 1-2, https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-creogn/reconnaissance-faciale-et-controles-preventifs-sur-la-voie-publique-l-enjeu-de-l-acceptabilite. See subsection 5.3.5.4 of the current report.*

891. *House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, 25 February 2015, HC° 734, n° 71, https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf: "Unlike a password or PIN code, an individual's biometric characteristic cannot easily be revoked or reissued if it is compromised. Giving evidence in 2006 to our predecessors, Professor Martyn Thomas stated that the theft of an individual's biometrics created a 'security nightmare' whereby somebody's biometrics were 'no longer available to them to authenticate themselves for the rest of their lives'".*

892. *See for example the case of France in subsection 7.1.2 of the current report.*

893. *In France, the data protection authority sanctioned the Ministry of home affairs for mismanagement of the fingerprint database: see subsection 7.1.2 of the current report.*

894. *In the same line, see Annemarie Sprokkereef and Paul De Hert, 'Ethical practice in the use of biometric identifiers within the EU', January 2007, Law, Science and Policy, 2007, Vol. 3, pp. 177–201 [p. 178], 1475-5335/07 ©2007 A B Academic Publishers, https://www.researchgate.net/publication/228369691_Ethical_practice_in_the_use_of_biometric_identifiers_within_the_EU. Authors refer to Anton Alterman, 'A piece of yourself: ethical issues in biometric identification', in Ethics and Information Technology, 5, 2003, p.139–150, https://www.academia.edu/32713161/A_piece_of_yourself_Ethical_issues_in_biometric_identification.*

895. *See subsection 4.1.2.8 of the current study.*

896. *Ayse Ceyhan, 'Les technologies européennes de contrôle de l'immigration : Vers une gestion électronique des "personnes à risque"', in Réseaux 2010/1 (n° 159), p.131-150, https://www.cairn.info/revue-reseaux-2010-1-page-131.htm.*

897. *Statewatch, EU action against terrorism: Council targets migrants and Muslims, 16 November 2020, https://www.statewatch.org/news/2020/november/eu-action-against-terrorism-council-targets-migrants-and-muslims/. The statement according to which non-discrimination must be ensured also appears in the EU legislation regulating borders management, without providing for concrete guarantees of application. See for example Regulation (EU) 2019/818, article 5, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.135.01.0085.01.ENG.*

898. *See for example Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 359, https://hal.archives-ouvertes.fr/tel-02439529.*

899. *Translated from French ("paradoxe accablant"): François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, Tallandier Essais, 2019, p. 35.*

900. *Translated from French: François Sureau, previously mentioned, p. 11.*

901. *See subsection 5.3.1.3 of the current study.*

902. *See subsection 4.1.2.11 of the current study.*

903. *Sébastien Van Drooghenbroeck and Cecilia Rizcallah, 'The ECHR and the Essence of Fundamental Rights: Searching for Sugar in Hot Milk?', 30 May 2019, German Law Journal (2019), 20, Cambridge University Press, pp. 904–923, p. 907, https://www.cambridge.org/core/services/aop-cambridge-core/content/view/594CA9F2A83DF4B52A1FB6B638339FB4/S2071832219000683a.pdf/echr_and_the_essence_of_fundamental_rights_searching_for_sugar_in_hot_milk.pdf. The authors refer to Janneke Gerards, EVRM Algemene Beginselen, 167 (2011).*

904. *See subsections 3.1.1 and 5.2.5 of the current study.*

905. *Noël Chahid-Nourai, who was Council member of the French Data Protection Authority (CNIL), stated the following, in relation to the French INSEE Code (N.I.R.) which is used as a national identification number: "if the N.I.R. had officially and operationally existed in 1943 and if we would have liked to select every people who were born in Poland because we thought they were potentially Jewish, we would have had the possibility to do it. If we want today to select also all the foreign people, it is sufficient to take the 99, which is the identification number for people who were born abroad, a category which widely covers the previous one. If we want to be more subtle and want to select, for example, to discriminate them, each person who was born in Iran, in Iraq or in Yugoslavia, we can do it (...). In a crisis time, it can be useful.." (translated from French): Noël Chahid-Nourai, speech to the panel 'Secret et nouvelles technologies', conference dedicated to professional secret organised by the "Conférence des bâtonniers", Les petites affiches, n° 122, 20 June 2001, p. 25 s.*

906. *See for example subsection 7.1.1.1 of the current study.*

907. *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine of 4 April 1997, Treaty n° 164, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=164. The Convention has been ratified by 25 Council of Europe Member States, including Romania (2001) and France (2012). The United Kingdom did not sign it.*

908. *See subsection 4.1.2.11 of the current study.*

909. *By signing the ECHR. On the positive obligation to ensure dignity, see for example ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, already mentioned, § 69 and 66: "States had a positive obligation to apply stringent and effective safeguards in order to ensure that their rights to exercise legal capacity were 'practical and effective' rather than 'theoretical and illusory'".*

910. *See subsection 5.2.4.2 of the current study.*

911. *See subsections 3.2, 4.1.1, and 5.2.4.2 of the current study.*

912. Vanessa Diaz, 'Legal challenges of biometric immigration control systems', in Mexican Law Review, Vol. 7, Issue 1, July - December 2014, p. 3-30 [p. 6], DOI: 10.1016/S1870-0578(16)30006-3, https://www.elsevier.es/en-revista-mexican-law-review-123-articulo-legal-challenges-biometric-immigration-control-S1870057816300063. The author goes on to say that "There is also an absence of public discussion of potential privacy right violations posed by linking centralized biometric immigration data with criminal databases and TBIF between nations and organizations".

913. European Forum for Urban Security, Citizens, Cities and Video Surveillance - Towards a democratic and responsible use of CCTV, June 2010, introduction p. 13, https://panoptykon.org/sites/panoptykon.org/files/cctv_publication_en_0.pdf: "since [the 11 September 2011] a plethora of means deemed useful in the fight against terrorism, including video surveillance, has been deployed at all levels. The questions of their effectiveness, of the appropriateness of the instruments used and their impact on freedoms in relation to objectives, especially over the long term, were secondary".

914. Giusto Catania (GUE/NGL), statement during the debate on the fight against terrorism before the European Parliament, 5 September 2007: "We have often said, and we say it firmly, and I think that we ought to say it again in this Chamber, that terrorism is the enemy of our civilisation, it is the enemy of the rule of democracy: terrorism is barbarity. Terrorist attacks represent a move from the rule of law to a primitive state. All this is true, but instead of focusing the debate on the reinstatement of the rules of democracy we have chosen to tackle the issue by restricting the rules of civil coexistence. We have chosen to fight on our adversary's home ground, to compete on violations of human rights, on military controls over the civilian population, on the negation of the key principles of democracy", https://www.europarl.europa.eu/doceo/document/CRE-6-2007-09-05-INT-3-014_EN.html?redirect.

915. See subsection 5.2.4.2 of the current study.

916. François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, already mentioned p.43 and footnote 24.

917. François Sureau, already mentioned, p. 43.

918. This type of totalitarianism might be called "authoritarianism". This term is used by authors to refer to political regimes that are less radical than totalitarianism in terms of limitation of freedoms (Michal Kim and Michael Schoenhals, '1. Introduction: Mass Dictatorship and the Radical Project for Modernity', and 3. Roger Griffin, 'Mass Dictatorship and the '"Modernist State"', in Michael Kim et al., Mass dictatorship and modernity, Palgrave MacMillan, 2013). However, totalitarianism and authoritarianism are considered to be part of the larger concept of "mass dictatorship", defined as a political regime that "sought to achieve the self-mobilisation of the masses for radical state projects [utilising] the utmost modern practices to form totalitarian cohesion and to stage public spectacles in the search for extremist solutions to perceived social problems" (Michal Kim and Michael Schoenhals, already mentioned).

919. See the introduction of the current study.

920. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 1.

921. See the introduction of the current study.

922. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 35, https://hal.archives-ouvertes.fr/tel-02439529

923. All quotations come from ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, appl. n° 53251/13, § 66, http://hudoc.echr.coe.int/eng?i=001-172134. See subsection 4.1.2.11 of the current study.

924. In an interview given with journalist Glenn Greenwald, Edward Snowden declared: "NSA, and the intelligence community in general, is focussed on getting intelligence wherever it can by any means possible. It believes, on the grounds of a sort of self-certification, that they serve the national interest": The Guardian, 'NSA whistleblower Edward Snowden: "I don't want to live in a society that does these sort of things" – video', 13 June 2013, https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video; see also Gabriel Rodriguez, 'Edward Snowden Interview Transcript FULL TEXT: Read the Guardian's Entire Interview With the Man Who Leaked PRISM', 6 September 2013, MIC, https://www.mic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism.

925. Patrick Gibert, 'L'évaluation de politique : contrôle externe de la gestion publique ?' in Revue française de gestion, 2003/6 (n° 147), p. 260, https://www.cairn.info/revue-francaise-de-gestion-2003-6-page-259.htm?contenu=article: "A certain idolisation of the state, a belief that public action systematically embodies the pursuit of the general interest, [and] an absolute confidence in the virtues of policies because they have been set up by legitimate authorities, proscribe the systematic examination of fact – which is evaluation – because such an examination is necessarily disrespectful, desacralising, demystifying" (translated from French). See also Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 365, https://hal.archives-ouvertes.fr/tel-02439529.

926. Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', Note du CREOGN, n° 43, September 2019, p. 4, https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-creogn/reconnaissance-faciale-et-controles-preventifs-sur-la-voie-publique-l-enjeu-de-l-acceptabilite. The author states that "recourse to facial recognition by law enforcement has the merit of being an enlightened choice of society" (translated from French).

927. The London Metropolitan Police has been using since 2016 a facial recognition technology, which is highly criticised, especially because tests revealed that "81% of matches made by the system were incorrect". However, Assistant Commissioner Nick Ephgrave declared: "As a modern police force, I believe that we have a duty to use new technologies to keep people safe in London. We are using a tried-and-tested technology. Similar technology is already widely used across the UK, in the private sector": Samuel White, 'London Metropolitan Police Will Deploy Live Facial Recognition

Systems', 27 January 2020, The Internet Protocol, https://internetprotocol.co/hype-news/2020/01/27/the-met-to-deploy-facial-recognition-cameras/.

928. ECtHR, 1st Sect., 23 March 2017, A.-M.V. v. Finland, already mentioned.

929. ECtHR, gr. ch., 4 December 2008, S. and Marper v. The United Kingdom, appl. n° 30562/04 and 30566/04, § 112, http://hudoc.echr.coe.int/eng?i=001-90051.

930. Translated from French: Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 55. The author refers to the statement from 120 members of the French Parliament in their referral to the Constitutional Council. The act of referral is availble at https://www.conseil-constitutionnel.fr/les-decisions/decision-n-2012-652-dc-du-22-mars-2012-saisine-par-60-deputes.

931. Translated from French: Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p.55. The author refers to a statement from François Pillet, reporter of the text before the Senate. By the end of the 19th Century, the same fear was expressed by the French public opinion in relation to the collection of photographs by public authorities. On this issue, see the introduction of the current report.

932. See subsections 4.1.1 and 5.1.5 of the current study.

933. Translated from French: Geneviève Koubi, 'Droit de résistance à l'oppression et désobéissance civique (III)', 16 March 2008, Droit cri-TIC, http://koubi.fr/spip.php?article51.

934. Translated from French: Jean-Marc Manach, 'La CNIL retoque (encore) le méga-fichier biométrique des « gens honnêtes', 17 March 2021, https://www.nextinpact.com/article/46457/la-cnil-retoque-encore-mega-fichier-biometrique-gens-honnetes.

935. See subsections 4.1.2.11, 4.1.2.12 and 4.1.3.5 of the current study.

936. See subsection 4.1.3 of the current study.

937. Translated from French : Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', already mentioned, p. 1-2.

938. See subsection 4.1.2.11 of the current study.

939. Friedrich A. Hayek showed that "in a society used to freedom it is unlikely that many people would be ready deliberately to purchase security [instead]. But the policies which are followed now are nevertheless rapidly creating conditions in which the striving for security tends to become stronger than the love of freedom": Friedrich A. Hayek, 'The Road to Serfdom', in The Road to Serfdom with The Intellectuals and Socialism, Institute of Economic Affairs, 2005, p. 69, https://cdn.mises.org/Road%20to%20serfdom.pdf. There is therefore a need, for citizens, to relearn the meaning of freedoms and the issues at stake. In the same line, John Torpey assumes that "the bureaucratic identification of subjects played a decisive role in the way subjects formed their identities as citizens and nationals": Albrecht Funk, 'John Torpey: The invention of the passport. Surveillance, Citizenship and the State', Crime, History and Societies, Varia, Vol. 5, n°2 - 2001, p. 157-158, n°1, also available at https://doi.org/10.4000/chs.745. On the prevention of totalitarianism through culture and self-identity, see also Michael J. Griffin and Tom Moylan, Exploring the Utopian impulse: Essays on utopian thought and practice, Peter Lang AG, International Academic Publishers, Bern 2007, p. 52.

940. See subsection 4.1.3 of the current study.

941. Friedrich A. Hayek, 'The Road to Serfdom', already mentioned, p. 69.

942. On the "renaming marketing strategy" which inspired current shifts in meaning, see Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 47 s., https://hal.archives-ouvertes.fr/tel-02439529.

943. David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 46 s., especially p. 57 ; See also François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, already mentioned, p. 10; Olivier Aïm, Les théories de la Surveillance – Du panoptique aux Surveillance Studies, ed. Armand Colin, 2020, p. 105.

944. François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, Tallandier Essais, 2019, p. 59.

945. François Sureau, afore-mentioned, p. 29-30.

946. Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 58; In relation to EU States that decided to suppress biometric data after having issued biometric IDs, see for example Jean-Marc Manach, La CNIL retoque (encore) le méga-fichier biométrique des « gens honnêtes », 17 March 2021, https://www.nextinpact.com/article/46457/la-cnil-retoque-encore-mega-fichier-biometrique-gens-honnetes

6

RECOMMENDATIONS

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

The impacts of biometric surveillance technologies on human rights require that practices be framed by laws that ensure the necessity and the proportionality of each implementation and each use, in relation to each purpose. This framework must also take into account risks to fundamental rights and freedoms, and implement appropriate corrective measures.

This implies that assessments of necessity and proportionality on the one hand and risk assessments on the other hand 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 balance are effective. Currently, it seems not to be the case, at the level of the European Union and at the level of some EU member states.[947]

Consequently, it appears crucial, first and foremost, to focus on the erosion of democratic structure and processes, and to ensure that the EU and the EU member states undertake the reforms necessary to restore effective checks and balances, and, more generally, to comply with the rule of law. In particular, parliaments must have an effective lawmaking power and must not be circumvented. Courts must be independent and their ruling must be respected and enforced. Data protection authorities must have effective supervisory and decision-making powers and their opinions must be respected and enforced as well. All these authorities and institutions must be adequately equipped and resourced to carry out their missions.

Assessments of compliance with the rule of law might be based on the *"Rule of Law Checklist"* provided by the Venice Commission of the Council of Europe[948]. In order to avoid *"risks of a purely formalistic concept of the Rule of Law"*[949], it is important that all the authorities and stakeholders to which the ECHR applies are also subject to the requirements of the rule of law. Authorities include intelligence services, as well as other authorities in charge of internal security. Even though their activities fall outside the scope of Union Law, both the EU and its member states bear responsibility for ensuring that they fulfil their commitment to enforce the ECHR. If the assessment of their activities cannot be envisioned at the EU level, it could be done at the level of the Council of Europe, which already issued recommendations in relation to digital surveillance by intelligence services[950]. Assessment of compliance with the rule of law should also target the activities of industrial actors that process personal data of individuals, in particular *"hybrid (State-private) actors and private entities which perform tasks that were formerly the domain of State authorities, or include unilateral decisions affecting a great number of people, as well as [...] international and supranational organisations"*.[951]

6.2 RESTORE THE CONDITIONS FOR DEMOCRATIC DEBATE

In a political democracy, states must ensure that the best contextual parameters are established in order to enable public debate. They must also ensure that contradictory opinions are taken into account.

This implies that states must avoid any paternalistic attitude from public authorities which result in making choices on behalf of citizens who raised their voices against a particular measure. 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. Such risk must be taken into account and cannot be dismissed unless contradictory evidence is provided. This must particularly be ensured in circumstances where public authorities are convinced of being right. Indeed, being convinced is not being right.

States must avoid any misrepresentations of reality, including the reality of the legal provisions that base human rights preservation. In this respect and in compliance with the ECHR, security must be presented as an exception to the principle of preservation of human rights. Legal instruments restricting freedoms with a view to ensuring security must be presented as such. Manipulation of opinion polling must be prohibited. The form of communication, itself, should not stigmatise minorities[952] and persons who question the legitimacy of proposals from public authorities[953]. This is the price for democracy and the power of words is not to be underestimated[954].

Codes of conducts[955] for political and public representatives might be envisioned in order to promote such *"ethics of communication"*[956]. Their aim would be to reach the ideal of *"mutual understanding and acceptance"*[957], which might be, according to the Venice Commission of the Council of Europe, *"the main challenge of modern societies"*[958].

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

Democracy requires that citizens be able to understand what legislation and practices really imply. One of the essential foundations of democracy is freedom of expression, which conditions a constructive exchange of ideas and opinions, and therefore the quality of public debate

[959]. States have a positive obligation to ensure the effectiveness of the freedom of expression[960]. This implies taking appropriate measures which enable citizens to gain the confidence that they can express themselves without fear[961]. This also implies providing citizens with the skills and critical attitude that enable them to face and understand the information they receive, including where this information is harmful to them[962]. Citizens' education and awareness must include the ability to distinguish between true and false information, the ability to understand the benefits and the risks of measures aiming at regulating their freedoms, and the ability to have a democratic and responsible attitude that respects the rights of others. This right to education is of particular importance and has been especially highlighted in several recommendations of the Council of Europe Committee of Ministers[963] as well as by the European Parliament[964].

A culture of human rights must be spread amongst political and public representatives, at national levels but also at the level of the European Union. Indeed, 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 the philosophy of preservation of human rights. Statements include the promotion of security as the first amongst freedoms, whereas security is only an objective that might – if necessary and proportionate – justify a duly vindicated limitation of freedom. This promotion is sometimes coupled with misrepresentations of facts[965], which feed the construction of *"prejudices and preconceived ideas"*[966] in the minds of the general public.[967] Statements also include shifts in meaning that aim to adopt restrictions of freedoms under the guise of protecting them. Practices include the circumvention of parliaments and the denial of decisions of supreme courts and data protection authorities, through the adoption of laws or regulatory acts that ignore their recommendations.[968] These practices and statements demonstrate a lack of a culture of democracy and human rights.

The spread of a culture of human rights could be articulated by including it in schools and other training curricula, including dedicated[969] to *"political, media and social elites"*[970]. It could usefully draw inspiration from the Council of Europe materials in relation to education to human rights[971].

The understanding of the letter and of the philosophy of preservation of human rights should also pervade Privacy and Data Protection Impact Assessments (respectively PIA and DPIA). Schematically, a PIA or a DPIA should include a necessity and proportionality assessment, as well as an analysis of risk to rights and freedoms[972]. Currently, most DPIA guidelines reduce the necessity and proportionality assessment to a check of compliance with the General Data Protection Regulation or the Police-Justice Directive. If such an approach might be sufficient in relation to low-risk data processing, this cannot be considered sufficient to assess the other personal data processing. In particular, this is not sufficient to assess laws, policies, and practices that are likely to impact absolute rights such as the right to hold a belief, the right to self-determination, and the right to human dignity.

6.4

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, for 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.[973]

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 others based on the three following criteria:

• The proximity of the data storage to the person concerned

Biometric identifiers should ideally be stored in a chip controlled by the person to whom the information relates, with small administrator rights. This would prevent most misuses. Storage in a central database on a third-party system should be prohibited in principle. Exceptions to this rule should not be allowed, unless duly justified. Admissible justifications might include the need to process fingerprints or images collected during criminal investigations, for the time of the related investigation and for the purpose of finding and prosecuting perpetrators of criminal infringements. Another admissible justification might be the need to keep track of persons who were condemned for a crime and who could re-offend, provided that this conclusion is based on reasons other than their condemnation. Any other creation of a central database should be, at a minimum, subject to the authorisation of the persons whose biometric information is involved. In contrast, local biometrics-based access control system, such as personal mobile phone unlock systems, may constitute legitimate and relatively secure usages, provided that the user is fully informed about the benefits and risks of the technology.

• The existing possibilities to reuse the biometric identifier in other purposes

Any system using biometric identifiers should ideally be designed to avoid, without the informed consent of data subject, the reuse of data, by other data controllers or in the pursuit of new purposes.

• The accuracy of biometric identifiers.

Many usages of biometry do not require a perfect unique world-wide match between a person and the stored biometric identifier. In these situations, identification or authentication could be limited to a decent probability that the technology recognises the person to be recognised, within a group of a greater or lesser size. Research should be encouraged in this respect.

Taking into account the emergency to safeguard crucial fundamental rights without which there can be no political democracy, any practice or technology that does not fulfil, at least, one of these three conditions must be prohibited. In a second phase, these three conditions should be ideally coupled together, unless duly justified contrary need, framed by effective guarantees against abuse.

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 needs.

(2) The collection and processing, by private entities, of biometric identifiers without the 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 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 the explicit and informed consent of the people concerned or involved.

In any and all situations, authorised technologies and services should be subject to a proper privacy impact assessment, and their operator 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.

947. See subsections 5.2.4 and 5.3.5 of the current study.

948. Council of Europe, European Commission for democracy through Law (Venice Commission), Rule of law Checklist. For further details, see subsection 2.3 of the current study.

949. Council of Europe, European Commission for democracy through Law, already mentioned, n° 15-16.

950. Joint statement from Alessandra Pierucci, Chair of the Committee of Convention 108, and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services, 7 September 2020, https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb.

951. Council of Europe, European Commission for democracy through Law, already mentioned, n° 15-16.

952. CNCDH, Rapport sur la lutte contre le racisme, l'antisémitisme et la xénophobie, Les Essentiels, 2016, p. 18 s., https://www.cncdh.fr/sites/default/files/les_essentiels_-_rapport_racisme_2016_1.pdf.

953. See subsections 5.2.4.2 and 5.3.5.6 of the current study.

954. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 46, https://hal.archives-ouvertes.fr/tel-02439529. The author especially refers to Victor Klemperer's works relating to the rhetoric used during the third Reich (Éric Heilmann in C. W. R. Webster et al., Video Surveillance: Practices and Policies in Europe, IOS Press, 2012., p.101).

955. Committee of Ministers of the Council of Europe, Appendix to Recommendation No. R (97) 21 on the media and the promotion of a culture of tolerance, 30 October 1997, https://rm.coe.int/168050513b. See for ex. n°4 of the Appendix.

956. Venice Commission, Blasphemy, insult and hatred: finding answers in a democratic society, Council of Europe publishing, Science and technique of democracy, March 2010, p. 31, n° 85. http://www.venice.coe.int/webforms/documents/?pdf=CDL-STD(2010)047-e. This formula is employed in relation to media and religious groups.

957. Venice Commission, Blasphemy, insult and hatred: finding answers in a democratic society, already mentioned, §87 p.31, http://www.venice.coe.int/webforms/documents/?pdf=CDL-STD(2010)047-e.

958. Venice Commission, already mentioned.

959. ECtHR, gr. ch., 22 October 2007, Lindon, Otchakovsky-Laurens and July v. France, § 51, appl. n°21279 and 36448/02, http://hudoc.echr.coe.int/fre?i=001-82846.

960. See subsection 4.1.2.3 of the current study.

961. ECtHR, 2nd Sect., 14 September 2010, Dink v. Turkey, appl. n° 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, §137, http://hudoc.echr.coe.int/eng?i=001-100384; ECtHR, Research report: positive obligations on member states under Article 10 to protect journalists and prevent impunity, Council of Europe/European Court of Human Rights, December 2011, p. 5, http://www.echr.coe.int/Documents/Research_report_article_10_ENG.pdf.

962. See subsection 4.1.2.3 of the current study.

963. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society, 13 May 2005, available in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, already mentioned, p. 288, http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information-Society/011_DeclarationFinal%20text_en.asp; In the same document see Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, p. 150 [p. 152, see also p. 153]; Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment, 27 September 2006, p. 124; Appendix to Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment, p 162, part III, especially p. 164 s.

964. European Parliament Resolution of 21 May 2013 on the EU Charter: standard setting for media freedom across the EU (2011/2246(INI)), n°30, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0203.

965. CNCDH, Rapport sur la lutte contre le racisme, l'antisémitisme et la xénophobie, Les Essentiels, 2016, p. 27, https://www.cncdh.fr/sites/default/files/les_essentiels_-_rapport_racisme_2016_1.pdf.

966. Translated from French. CNCDH, Rapport sur la lutte contre le racisme, l'antisémitisme et la xénophobie, Les Essentiels, 2016, p. 27, http://www.cncdh.fr/sites/default/files/les_essentiels_-_rapport_racisme_2016_1.pdf.

967. Estelle De Marco (ed.), Definition of illegal hatred and implications, Deliverable D2.1b (final report), 30 September 2017, MANDOLA EU project - GA n° JUST/2014/RRAC/AG/HATE/6652, subsection n° 6.2.3, http://mandola-project.eu/publications/.

968. See subsections 5.2.4 and 5.3.5 of the current study.

969. Committee of Ministers of the Council of Europe, Appendix to Recommendation No. R (97) 21 on the media and the promotion of a culture of tolerance, 30 October 1997, https://rm.coe.int/168050513b (see for ex. n°1 of the Appendix).

970. Translated from French: CNCDH, Rapport sur la lutte contre le racisme, l'antisémitisme et la xénophobie, 2016, p. 8, http://www.cncdh.fr/sites/default/files/les_essentiels_-_rapport_racisme_2016_1.

971. *Council of Europe, Publications, in Democracy, Education, https://www.coe.int/en/web/education/publications.*

972. *See subsections 2.4 and 5.1 of the current study.*

973. *See subsections 4.1.1 and 5.3.5 of the current study.*

7

CASES STUDIES

7.1 FRANCE

7.1.1 STATE OF USE OF SURVEILLANCE TECHNOLOGIES

1) CURRENT OFFLINE USE, BY PUBLIC AUTHORITIES, OF BIOMETRIC AND BEHAVIOURAL MASS SURVEILLANCE TECHNOLOGIES

Identity documents

France issues several secured identity documents, whose delivery has been administered by the National Secure Credentials Agency (ANTS) since 2007. These documents include passports, identity cards, visas, and residence permits.[974] Among these documents, several include a chip which stores biometric information.

Biometric passports have been delivered since June 2009975 and biometric identity cards since August 2021976. Both include an electronic component which stores the holder's civil status, address, size, eye-colour, digitalised facial image, and fingerprints, reduced to two fingers[977]. However, citizens can refuse the digital processing of their fingerprints. In such case, fingerprints are kept on a paper copy[978].

In addition, such data is stored in a centralised database called *"File of secure electronic documents"*(TES)[979]. This file includes the above-mentioned information in addition to the name, birth information, sex, details of descent, and a digital image of the signature. This file also includes the holder's email address and telephone number, where the data was collected within the framework of certain situations, which are linked to the delivery of the identity document.[980] Such data is stored for fifteen years as a principle, and for ten years where data relates to a passport requested by a minor.[981]

The EU legislation

[982] makes it mandatory to destroy biometric identifiers after the biometric ID card has been issued, unless otherwise required for the purpose of necessary and proportionate processing, established at the national level in accordance with Union and national law. The French legislation's purposes are the establishment, delivery and invalidation of identity documents on the one hand, and the prevention and detection of falsification and counterfeiting of identity documents on the second hand[983] In addition, the decree that establishes the biometric database grants access to digitalised facial images, as well as to a series of information such as sex, filiation, eye-colour, email, to – non-exhaustively - law enforcement and specialised intelligence service agents in charge of the prevention and repression of threats to fundamental interests of the nation and of terrorism[984]. Moreover, the fight against identity theft has been added to the list of purposes of the French legislation, by a decree adopted in order to implement the EU regulation on the strengthening of identity cards.[985] Consequently, the *"strict necessity"* of the French processing to reach such purposes can be questioned, taking into account that other countries having the same needs have chosen to follow the EU Regulation and to delete biometric identifiers after identity cards are issued.[986] The legitimacy of the legal basis for this French biometric database can also be questioned. Indeed, it has been created by means of a decree. However, on such an important issue, the parliament should have been seized, based on article 34 of the Constitution which grants the legislator the power to *"determine the rules concerning [...] civic rights and the fundamental guarantees granted to citizens for the exercise of their civil liberties"*[987]. The French Data Protection Authority issued the same concern[988].

Video-surveillance

In relation to video-surveillance, the exact number of cameras deployed in France is unknown. Public-driven cameras are mostly implemented by cities without a reporting system being established[989]. Cities have been encouraged to do so by the government starting in 2007, within the framework of a *"vigorous national promotional campaign"*[990].

Moreover, local authorities may receive important financial support within that framework, notably from a dedicated Interdepartmental Fund.[991]

However, available figures show that Paris commands 42,500 cameras for a ratio of 3.84 cameras for 1,000 inhabitants.[992] *"Control centers"* are also under deployment in order to *"centralise video streams from several stakeholders"* such as local authorities and public transportation.[993]

There is in principle very little public use of CCTV with facial recognition. This is due to the combination of three factors: the lack of a clear legislation basing facial recognition in publicly accessible places, the CNIL's opposition to such practice outside appropriate legal framework, and a strong opposition from civil society.[994]

This being said, it seems that facial recognition is used by law enforcement and intelligence agencies, at least in a certain extent, and this takes place in a complete lack of transparency. For example, in 2016, Safran Identity & Security announced that the French National Police was *"using its MVI solution (Morpho Video Investigator) to analyse large amounts of video in a short amount of time"*, for the purpose of fighting terrorism and ensuring public security.[995] However, in 2019, the Ministry of Home Affairs, Christophe Castaner, declared regret that facial recognition was not available. It is reported that he exclaimed: *"let's not be prudish as gazelles!"* in order to support the dissemination of the technology. He gave a practical example where investigators had to look at each image of a video-surveillance system themselves in order to localise the author of an attack, whereas facial recognition would have helped to arrest him more easily and sooner.[996] As of February 2020, a series of law enforcement and government-affiliated agencies used, without managerial oversight and outside any legal framework, a software aiming to perform facial recognition based on photographs collected on social networks by Clearview AI, which was the provider of this solution[997]. French law enforcement agencies were reported to be involved, and the media BuzzFeed News describes that *"internal data [listing] employees associated with the office as having run more than 400 searches"*. However, France's Ministry of Home Affairs told the same media *"that they had no information on Clearview"*.[998] In October 2020, the Newspaper Next INpact reported that law enforcement agencies already used facial recognition massively in order to ease investigations. Next INpact specified that the primary database to be used is the TAJ, which contains 8 million photographs relating to, amongst others, persons suspected of committing a penal offence and victims[999]. Almost 600,000 requests for comparison with this file would have been made in 2019 and 2020.[1000]

In 2021, the Ministry of Home Affairs signed a contract in order to equip law enforcement with 30,[000] body-worn cameras, manufactured by the enterprise Motorola (VB400 model)[1001]. The aim is to record evidence in case of police intervention and the French President Emmanuel Macron announced, in July 2020, his wish to generalise their use[1002]. At this stage, these camera are not used for biometric surveillance purposes, but the Motorola model allows to send live images that could technically be monitored using biometric or behavioural recognition systems, directly or in a second phase. Mobile facial recognition is in addition non excluded from the plans of the Ministry of Home Affairs.[1003]

Next INpact also reports that, each month, new airports and border crossings are equipped with facial recognition technology.[1004]

Surveillance practices during the Covid-19 Pandemic

During the Covid-19 pandemic, the use of drones by police forces has been revealed. The aim was to verify the respect for lockdown measures, to monitor public protests, to assist investigations, and to monitor some behaviours such as urban rodeos.[1005] The French Data Protection Authority (CNIL) sanctioned the Ministry of Home Affairs for these operations. The Authority stated schematically that operations should have been based on a law specifying appropriate safeguards, after completion of an impact assessment. The CNIL also highlighted that transparency towards citizens was commanded.[1006] The Council of State also ruled that the use of drones during the pandemic did not comply with the data protection legislation.[1007]

During the pandemic, other questionable measures have been reported, such as the experiment of a facial recognition software in a Parisian underground station. Six cameras could identify citizens who did not wear a facial mask. The CNIL condemned and put an end to the experiment[1008]. In March 2021, a decree authorised public transport operators to use intelligent cameras in order to measure the rate of

mask-use. The CNIL recalled that such technology *"is not intended to process biometric data and does not constitute a facial recognition mechanism"*[1009].

Other biometric and behavioural recognition experiments

Several other experiments of biometric and behavioural recognition were reported. Next INpact details several of them.[1010] For example, the project VOIE (Open and Integrated Video-protection) aimed to follow individuals and to analyse videos within the framework of legal requisitions. It involved the Paris Police Headquarters, French public transporters, and technology providers Thales, Morpho (which became IDEMIA), and Deveryware. The CNIL prohibited such live experiment in publicly accessible places. Another project, called S UCRE (Safety and Security of UrbanCrowded Environments) was dedicated to crowd control and included inter alia behaviour prediction and detection. It was driven by IDEMIA, and partners included Deveryware and the Paris Police Headquarters. It received a funding of EUR 1 million from the French National Agency for research (ANR).[1011]

Another illustration is the French city of Nice. In 2019, it experienced facial recognition during the carnival, with a view to detecting persons already registered in a database, with the consent of persons involved.[1012] During the same year, the same city envisioned experimenting a system capable of detecting travellers' emotions in public transport, with the aim of identifying potential suspects before an incident occurs[1013]. This project is reported as being abandoned due to a technical issue.[1014]

E-administration

In May 2019, a decree[1015] established a mechanism of *"online certified authentication on mobile phone"*, also called ALICEM. As clearly explained by the specialised journalist Marc Rees, this software enables individuals to create a *"digital identity"*[1016] which will be used to access a number of private and public services such as using public transportation[1017].or to access pornographic websites[1018]. The system is based on a facial recognition system, which will be interconnected with the TES database in order to collect the information it requires. In addition to information already evoked (such as the name, sex, birth information, eye-colour, digital photograph, and e-mail), other information will be gathered, such as the photograph taken by the user, the name of the service provider, the nature of the service used, and the delivery date. Some information will be stored on the smartphone while other will be stored in a centralised database. This decree does not take into account all the recommendations the CNIL issued in 2018[1019], when it was consulted before the adoption of the decree. Especially, the CNIL recalled the need of a data protection impact assessment and highlighted that the ALICEM application will only be available on Android devices, provided they are not *"rooted"*[1020]. The CNIL also recalled that the GDPR imposes free and informed consent of users, who should be capable of choosing alternative identification means but of a biometrical nature. In addition, the CNIL considered that the government did not demonstrate that such data processing was *"necessary for reasons of substantial public interest"*, as required by Article 9, g of the GDPR, which commands that alternative authentication means be proposed. On 15 July 2019, La Quadrature du Net, a French association advocating digital freedom, contested the ALICEM decree before the Council of State[1021]. A researcher also highlighted the danger of addiction to such usages[1022].[1023]

2) OTHER USAGES OF SURVEILLANCE TECHNOLOGIES

A. PUBLIC USAGE OF SURVEILLANCE TECHNOLOGIES

Intelligence services

French intelligence services include several agencies: the General Directorate for Internal Security (DGSI)[1024], the General Directorate for External Security (DGSE)[1025], the Armed Forces Ministry's intelligence service (DRSD)[1026], the Directorate of Military Intelligence (DRM)[1027], the National Directorate of Intelligence and Customs Investigations (DNRED)[1028], and the TRACFIN service in charge of the action against illicit financial circuits[1029].

The powers of intelligence services are mainly regulated by the Internal Security Code, which grants them extended powers with more than questionable proportionality. Essentially, the purposes which motivate powers are sometimes as vague as *"national defence"* or *"prevention of organised crime and delinquency"*[1030]. The scope and

the modalities of exercise of certain powers also suffer from legal ambiguity and uncertainty. The necessity of these powers, especially in terms of efficiency, has not been not demonstrated.[1031] As a result, the power of access of intelligence services may concern the data of any individual, as well as the whole of their *"electronic life"*.[1032] This must also be read in conjunction with article 40 of the French penal procedure Code, which includes a provision that commands any public officer, who learns about a penal infringement at the occasion of their missions, to inform the public prosecutor about it. Therefore, this provisions authorises, in practice, the use in any kind of penal proceedings, of evidence whose collection was exclusively authorised in the pursuit of a crucial objective. This contradicts article 8 2 of the European Convention on Human Rights.[1033]

Other administrative authorities

The specialised journalist Olivier Tesquet highlights[1034] that in 1974, the wish of the state to interconnect several databases, relating to citizens, with a unique identifier, raised a wave of protests by society, which led to the adoption of the first data protection law, in 1978. From then, French authorities multiplied databases relating to the French population. In 2018, their number was 106. Some of these files were legalised after having been used for years in a complete lack of transparency, such as the JUDEX file, which contained in 2005 more than *"4.7 millions of [...] suspects, victims, convicted persons, innocents who had the charges against them dropped or who have been acquitted"*[1035]. One of the last processing initiatives is the database of secured digital identity documents (TES), which will gather the biometric identifiers of the whole population but the children, and which has been qualified by a parliamentarian as *"monster file"*[1036] . This file *"is largely inspired"*[1037] from a former governmental project declared unlawful by the Constitutional Council in 2012. Called by a member of the parliament the *"file of honest people"*[1038], this 2012 project stirred one hundred and twenty French parliamentary members who feared *"the collapse, in the future, of any possibility of effective exercise of the fundamental right to oppression, corollary to individual freedom itself"*[1039]. However, the TES was established in 2016 by decree. The CNIL regretted this circumvention of the parliament[1040]

The TES file was afterward unsuccessfully[1041] challenged before the Council of State, by La Quadrature du Net and the Human Rights League[1042].

Despite the sensitivity of the processing, by public authorities, of citizens' personal data including data of a biometric nature, and despite the French administration's actual experience in that field, it appears that these files are not always appropriately managed. The specialised journalist Jean-Marc Manach reports that on 24 September 2021, the CNIL sanctioned the Ministry of Home Affairs for mismanagement of the FAED fingerprints database. The CNIL observed that more than 2 million records have been kept beyond the maximum conservation period, which is 25 years, some of them dating back to 1962. The CNIL also noted that 7 million paper records are stored without any legal basis. It highlighted that some records concerned people who had won acquittal and that, in all cases, persons concerned have not been informed. The CNIL also noted that insufficient security measures are in place, because of the use of a weak password.[1043]

B. PRIVATE USAGE OF SURVEILLANCE TECHNOLOGIES

According to studies, the French security market is growing. The use by families is still relatively weak[1044] and the market targeting professionals is leading: *"Requested video-surveillance systems are custom-made according to the need of each sector"*.[1045]

These systems might include biometric recognition. For example, it is reported that French supermarkets are deploying behavioural recognition in order to detect thefts. It is the case of Carrefour, Monoprix, Super U and Franprix. Providers for these technologies include Anaveo and its software «*SuspectTracker*», the Parisian start-up Oxania and its software «*Retail Solutions*», and the Parisian start-up Veesion. 1046 The latter announces that it equips more that 120 shops in France.[1047] Some banks are also reported as developing biometric authentication. In particular, La Société Générale declares using a technology provided by IDEMIA, which is used at border-crossings.[1048]

Several educational institutions are also tempted by facial recognition technology. In September 2019, two French high schools sent a request for advice to the CNIL. They wanted to experiment with facial recognition to enable access to the school premises. The CNIL considered that such authentication mechanism was neither necessary nor proportionate.[1049] Other educational institutions implement biometric technology, such as hand-

contour recognition, to authorise access to the school canteen. The CNIL recalled that the GDPR requires collecting parents' consent beforehand and that refusal on their part must lead to the provision of alternative access means[1050].

3) POLITICAL STANDING IN RELATION TO THE USE OF MASS SURVEILLANCE TECHNOLOGIES

The public administration specialist Guillaume Gormand[1051] reports that from 2005 on, under the presidency of Nicolas Sarkozy, the government deliberately created *"an artificial atmosphere of fear"*[1052] through *"a rise in national security discourse"* and the *"use of a particularly clever rhetoric designed to instil fear in the population and to call on citizens to choose between the cause of 'victims' and the cause of 'thugs'"*[1053]. This included the manipulation of public opinion polls in order to put forward the claim that citizens were expecting more security[1054].

In 2008, to avoid accusations of *"security drift and of generalised surveillance"*[1055], a *"semantic reversal"* led to replace the expression *"video-surveillance"* with the expression *"video-protection"*. This was also reflected in legislation in 2009. The French Ministry of Home Affairs even created a logo with this new terminology, accompanied with a slogan stating *"security at the service of freedom"*[1056].

The rhetoric of presenting security as an undisputable need that supersedes all freedoms has largely been constant ever since.[1057] The need to widely implement biometry as the best means to ensure security follows the same path. The political rhetoric is up so high that it is very difficult to oppose these views without being considered illegitimate and irrelevant.

An illustration is given by some members of the French Senate who declared that data collection and data interconnection, by the state, is a safeguard for civil liberties. They suggested that data protection is a *"French taboo"* and they questioned the relevance of being privacy-protective towards the state *"whereas Internet providers 'have a certain number of our data'"*.

[1058] Another perfect illustration, reported by Marc Rees[1059], is a statement from Renaud Muselier, president of the southern region. He made it when the CNIL refused to authorise the experimenting of facial recognition to enter some school premises, which the CNIL deemed unnecessary and disproportionate. Renaud Muselier declared that the CNIL *"is blocked in the* 20*th century"* and has a *"dusty ideology"*. The parliamentarian ric Ciotti made similar remarks. Christian Estrosi, Mayor of Nice, also regretted the CNIL's decision and put forward the *"real relevance"* of biometry to security enforcement. Éric Ciotti also put forward this argument. However, the added value in terms of security was not demonstrated.[1060]

The French government also has a long tradition of short-circuiting debates through the adoption of decrees or of emergency ordinances instead of laws, as it has been shown in previous sections of the current report. Moreover, legal instruments are sometimes vague in their formulation, which enables several interpretations and especially those that authorise the implementation of biometry. La Quadrature du Net shows for example how the stacking of a law and of two decrees enable live facial recognition of public protests to happen, while this is not formerly announced[1061]. In relation to the National Commission for Video-Surveillance, when this commission was first established to control video-surveillance as implemented by the public sector, Guillaume Gormand explains that *"its role was sufficiently vague in order to give free rein to the video-surveillance legitimation and promotion campaign"*.[1062]

Worse, governmental legislative proposals or decrees often disregard previous contrary opinions from parliamentary members and legitimate authorities such as data protection authorities and supreme courts.[1063] The more patent illustration of this is the TES biometric file, created by decree after a law proposing it was considered unconstitutional by the Constitutional Council.

François Sureau shows that such disregard of counter-power is further likely to prompt parliamentary members to adopt proposed laws in order to avoid being deprived of the possibility to discuss further laws of the same kind if they raised an opposition[1064]. This takes place in a context where the establishment of the five-year presidential mandate has suppressed, in practice, the opportunity of a parliamentary opposition[1065].

Another governmental habit is to adopt intrusive measures and to extend their scope of application afterwards in the pursuit of other objectives.

This has been shown in relation to the TES data processing[1066] and is regularly the case of measures which aim to combat terrorism[1067].

The clear will of the government to develop artificial intelligence and biometric recognition in publicly accessible places is also illustrated by a Home Affairs white paper[1068], declarations from the Minister of State for the Digital Sector[1069] and from law enforcement[1070], as well as the purchase of drones whereas currently no legal framework authorises their use[1071].

However, it seems that it originally comes from the impulsion of the biometric industry. Indeed, Guillaume Gormand argues that video-surveillance advocates strived to legitimise its use *"by addiction and habit"* on the part of both citizens and public policy actors[1072]. In 2019, Next INpact observed that *"behind the scenes, industrials push for France to not lag behind and Home Affairs is sensitive to arguments"*.[1073] An investigation from France Culture also argues that facial recognition technology makes progress in the shadows of public debates and that some enterprises *"are positioning themselves"*, targeting the 2024 Olympic games which lead to a market of EUR 7 billion[1074].

7.1.2 LEGISLATION REGULATING MASS SURVEILLANCE TECHNOLOGIES

The 1789 French Declaration of Human and Citizens Rights is included in the so-called French *"Constitutionality bloc"* and has therefore constitutional value[1075]. The Constitution so defined protects all the rights enshrined in the ECtHR, even though it is sometimes not that clear and the protection results from a decision by the Constitutional Council. For example, the right to private life is protected by the French Constitutional Council on the basis of articles 2 and 4 of the 1789 Declaration. The right to freedom of expression is protected under article 11 of the 1789 Declaration. The prohibition of discrimination is declared in article 1 of the 1789 Declaration.

In addition, France adhered to the European Convention on Human Rights, which came into force in May 1974[1076]. The Convention is directly integrated into the local system by the Constitution, as its article 55 states that *"Treaties or agreements duly ratified or approved shall, upon publication, prevail over Acts of Parliament, subject, with respect to each agreement or treaty, to its application by the other party"*.[1077] The Convention is therefore of infra-constitutional but of a supra-legal force, including on laws adopted subsequent to the Convention[1078].

The General Data Protection Regulation (GDPR) and the Police-Justice Directive which applies to judicial and police data processing, were implemented in the French Data Protection Law of 19781079. The French Data Protection Authority, named CNIL, enforces their respect.[1080]

The powers of intelligence services are regulated by the Internal Security Code (ISC), under the supervision of the Commission for the control of intelligence techniques (CNCTR).[1081]

Video-surveillance, called *"video-protection"*[1082] in order to foster acceptability[1083], is also regulated in the Internal Security Code[1084]. Implementation of video-surveillance is subject to authorisation, and people must be informed of the existence of video-surveillance systems.[1085] However, in practice, anyone who walks in the streets of cities such as Paris or Montpellier cannot see any public disclaimer in this regard (except at some town entry points), and cameras are not easily detectable[1086]. Mobile cameras are also regulated in the Internal Security Code[1087]

A national commission for video-protection exercises advisory and assessment missions towards video-surveillance[1088]. Its opinion does not bind public authorities at all times, in particular in situations of terrorist emergency.[1089] Other authorities and entities have some supervisory powers in relation to the activities of intelligence services. These include the CNIL[1090], which can control most of intelligence and police files[1091]. The Commission for the secrecy of national defence also has reasonable supervisory powers, but its opinion generally does not bind the government.[1092] Some other authorities can also exercise some scrutiny, at least in the form of information provided to the general public. These are the Commission for Access to Administrative Documents (CADA), the National Consultative Commission for Human Rights (CNCDH) and the national Commissioner for Human Rights (D fenseur des droits).[1093]

7.1.3 CIVIL SOCIETY RESPONSES

As shown in previous subsections of the current study, several philosophers, journalists and legal authors regularly warn about the danger of the rise of a society where the individual is the subject of a disproportionate control, in particular in relation to the biometric identification of all citizens and residents, and about risks posed by facial recognition in public and private places. This is also the case of parliamentarians and several independent authorities. In particular, the CNIL published a document where it calls for a debate *"appropriate to what is at stake"*.[1094]

Several NGOs and associations are also active in France, in particular the Human Right League[1095] and La Quadrature du Net[1096]. They regularly inform the population about the public measures they deem disproportionate and challenge them before courts, often successfully[1097]. More recently, several organisations have created the *"Technopolice"* platform[1098], which aims to *"document, as rigorously as possible, the deployment of surveillance projects across the country, and build together tools and mobilisation strategies that make it possible to defeat them"*[1099]. The association La Quadrature du Net clarifies that *"the issue is to succeed in organising local resistance, binding together initiatives so that they can feed into each other"*[1100].

The press is also very active in informing citizens. Several newspapers give great importance to surveillance issues, such as Next INpact and Le Monde.

Civil society's opposition and the CNIL's actions have slowed down the implementation of biometry. However, the opposition from civil society does not seem to extend to the whole population. Indeed, the public communication aiming to instil fear in the general public and increase the acceptability of surveillance technology, especially by presenting it as a key to freedom[1101], met with a certain degree of success. Friedrich A. Hayek and Fran ois Sureau both perfectly showed that where security policies are followed, they create the *"conditions in which the striving for security tends to become stronger than the love of freedom"*[1102], and that each time a law is contrary to the philosophy of preservation of freedoms, this very philosophy is a bit more lost as a value[1103] - and needs to be relearned.

7.2 THE UNITED KINGDOM

7.2.1. STATE OF USE OF SURVEILLANCE TECHNOLOGIES

1) CURRENT OFFLINE USE, BY PUBLIC AUTHORITIES, OF BIOMETRIC AND BEHAVIOURAL MASS SURVEILLANCE TECHNOLOGIES

Identity documents

The United Kingdom does not issue identity cards. Since the Second World War, identity cards have been abolished and new attempts to reintroduce them failed until the 2006 Identity Card Act was adopted against a backdrop of protests[1104]. In 2010, the new government proposed to scrap this scheme, and, in December 2010, the Identity Documents Act 2010[1105] repealed the Identity Cards Act of 2006. Consequently, the Secretary of State does not issue ID cards any more (art. 2 of the Act) and had to ensure the destruction of *"all the information recorded in the National Identity Register"* before the end of the period of two months after the act passed (art. 3 of the Act).

However, the United Kingdom implemented passports with a digitised image, stored in a chip in the passport from 2006 onward. This image is also collected in the central database of Her Majesty's Passport Office (HM Passport Office), together with other information necessary to issue the passport (such as birth information, gender and, if recorded digitally, signature).[1106] The HM Passport Office is

"the official government service to British citizens at home and abroad" and it declares that its priorities are to *"contribute to achieving the Home Office's priorities of securing [...] borders and reducing immigration, cutting crime and protecting [...] citizens from terrorism"*.[1107]

The Home Office also issues *"biometric immigration documents"* (BID) which are biometric residence permit (BRP) and short stay permits (SSP).[1108] People who apply *"for leave exceeding* 6 *months must also apply for the issue of a BRP"* whereas SSP cover, since 2015, *"people applying from within the UK to extend their leave to a total of* 6 *months or less"*.[1109] The biometric *"information is stored on the immigration and asylum biometric information system (IABS) held by the immigration fingerprint bureau (IFB)"*.[1110]

Since Brexit and *"the end of the transition period on 31 December 2020, the United Kingdom no longer has access to the Europol Information System or to the system that allows Member States to search data in Analysis Projects on a hit/no hit basis. [...] On 1 January 2021, eu-LISA disconnected the United Kingdom from the Schengen Information System and deleted all of its alerts on natural persons"*.[1111] However, it appears the United Kingdom made *"illegal copies"* of the database and is suspected to have shared it with the US government and US companies.[1112]

Video-surveillance

In relation to video surveillance, the exact number of cameras deployed in the United Kingdom is not reported. However, available figures show that London installed more than 691,000 cameras for a ratio of 73.31 cameras for 1,000 inhabitants, which had it taking the lead in that area, when the UK was within the European Union.[1113] There seems to be no extensive public use of CCTV with facial recognition[1114] - at least officially, especially because facial recognition is contested by civil society and has been ruled unlawful. In 2017 and 2018, the South Wales police implemented automated facial recognition technology. In 2020, the Court of Appeal found this system contrary to article 8 (^{2}) of the ECHR[1115], after the High Court issued a contrary decision[1116].

The London Metropolitan Police has been testing since 2016 a live facial recognition technology, and announced in 2020 its intention to deploy it across London. This practice is highly criticised, based on the respect due to privacy. Tests revealed that *"81% of matches made by the system were incorrect"*. However, Assistant Commissioner Nick Ephgrave declared: *"As a modern police force, I believe that we have a duty to use new technologies to keep people safe in London. We are using a tried-and-tested technology. Similar technology is already widely used across the UK, in the private sector"*.[1117] Currently, the technology is active and aims *"to help tackle serious violence, gun and knife crime, child sexual exploitation and help protect the vulnerable"*[1118].

The London Metropolitan Police also equips officers with body-worn cameras, manufactured by the enterprise Axon[1119]. These cameras aim *"to capture both video and audio evidence when they attend all types of incidents"*[1120]. Other public safety forces also use such cameras. For example, the Lancashire Constabulary is reported to deploy VB400 body-worn cameras from the American company Motorola[1121].

Surveillances practices during the Covid-19 Pandemic

Finally, it was reported that during the Covid-19 pandemic, police forces used drones *"throughout the country [...] to monitor and track protests, including those against the authoritarian lockdowns imposed by the government"*.[1122]

More globally, research on the use of biometric data by 96 countries[1123] observes that *"the country with the worst number of facial recognition technologies in use/being developed for the pandemic is the United Kingdom"*. It considers four possible facial recognition developments: *"the possible introduction of facial recognition in "*quarantine hotels*" to make sure people remain in isolation, the use of health passports to create digital certificate/immunity passports, the development of high-resolution cameras that can detect fevers and carry out profiling, and the potential use of biometrics (DNA/fingerprints) upon entry into the country and the extension of their retainment"*.

In particular, The Guardian[1124] revealed that the National Health Service (NHS) App, which serves during the Covid-19 pandemic as a vaccine passport, operates facial recognition in opaque conditions. This app also enables *"users to view their health records, fill repeat prescriptions, and book medical service appointments"*.[1125] It may also be asked *"for entry to events such as football matches"*

1126. The app may verify *"citizens' identities by having them upload a video of their face, which is used to compare against the photo registered with their government identification"*, with a possibility to opt-out.[1127] The app *"also asks users to upload their date of birth, postcode, phone number and a photo of either their passport or driving licence during the sign-up process"*[1128]. The Guardian reports that the contract between the NHS and the company that operates the facial recognition, called iProov, has not been publicly disclosed, neither passed a privacy risk assessment, both for security reasons. Law enforcement access to such data has not been excluded, whereas an expert in surveillance law *"said such information was likely to be desirable to UK and foreign intelligence services"*. Opacity also surrounds the relationship between the London-based iProov and the government. For example, iProov *"previously won contracts with HM Revenue & Customs and worked on the Home Office's "*settled status*" Brexit scheme for EU citizens who wish to remain in the UK"*.[1129]

E-administration

Despite these criticisms that have not all received answers, the government announced, in October 2021, its wish to introduce, in 2022, a facial recognition app that *"will enable citizens to access over 300 government services through their smartphones. The app will either use facial recognition or fingerprint scanning to verify the user"*.[1130] Stephen Barclay, the Chancellor of the Duchy of Lancaster, declared *"people rightly expect government to be data-driven and digitally literate, and this will be a priority for me in my new role"*[1131] of head of the Cabinet Office. This statement has not been supported by further evidence, whereas some criticism already questions whether this project is not *"'yet another black hole' for taxpayers money»*. Indeed, a project of the same kind failed in the past and it demonstrates, according to a 2019 parliamentary report, *«many of the failings we see all too often on large government projects: expectations were over-optimistic from the start, key targets have been badly missed and results simply not delivered"*.[1132]

2) OTHER USAGES OF SURVEILLANCE TECHNOLOGIES

A. PUBLIC USAGE OF SURVEILLANCE TECHNOLOGIES

In the United Kingdom, each citizen has a national insurance number.[1133]

Intelligence services

The United Kingdom intelligence services have a long tradition of collecting information on their citizens and residents, and of information sharing with other services. The United Kingdom Intelligence services are the Security Service (MI5, in charge of national security[1134]), the Intelligence Secret Service (SIS or MI6, *"responsible for gathering intelligence outside the UK in support of the government's security, defence, foreign and economic policies"*[1135]), and the Government Communications Headquarters (GCHQ, which *"provides intelligence, protects information and informs relevant UK policy to keep society safe and successful in the internet age"*[1136]).

Since 5 March 1946, a British-US Communication Intelligence Agreement has governed *"the arrangements between the British and United States authorities in relation to the exchange of intelligence information"*[1137]. This agreement was marked *"Top Secret"* until its transfer to the National Archive.[1138] Since then, other allegations have been made with regard to possible data exchange with *"foreign intelligence and other law enforcement agencies"*. The data concerned would have been collected *"over years, even decades"*, and would cover *"personal social media data"* that *"has reportedly been categorised into biographical data, financial activities, travel, and more"*.[1139]

In 2013, Edward Snowden, former contractor for the National Security Agency (*"NSA"*) of the United States, revealed the PRISM[1140] and Upstream[1141] programs, and the existence of information exchanges between the UK and the USA.[1142] Especially, the GCHQ obtained information from the USA on UK nationals and residents. 1143 In addition, the GCHQ *"was operating two major processing systems for the bulk interception of communications"*.[1144] This was especially established by the UK Investigatory Powers Tribunal, which observed that, before 2015, the collection of bulk data relating to individuals took place without *"statutory oversight"*[1145] and was

therefore unlawful, based on article 8 of the ECHR[1146]. Intercepted data included *"considerable volumes of data about biographical details, commercial and financial activities, communications and travel"*, and especially *"the 'who, when, where and how' of both telephone and internet use"*, together with locations.[1147] In 2021, the ECtHR considered that these practices were not surrounded by sufficient *"'end-to-end' safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse"*, targeting in particular *"the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation"*. These weaknesses *"concerned not only the interception of the contents of communications but also the interception of related communications data"*.[1148] Practices of bulk data collection are still active[1149], based on a new legal framework (the Investigatory Powers Act 20161150), which is still criticised for being disproportionate[1151] and might be challenged before a court again[1152].

At the same time, in 2016, the GCHQ admitted the use of *"Computer network exploitations"* (CNE) - *"or in its colloquial form 'hacking'"*.[1153] This covered *"the obtaining of information from a particular device, server or network"*, *"the creation, modification or deletion of information on a device, server or network"*, *"the carrying out of intrusive surveillance"*, *"the use of CNE in such a way that it creates a potential security vulnerability in software or hardware, on a server or on a network"*, and *"the use of CNE in respect of numerous devices, servers or networks, without having first identified any particular device or person as being of intelligence interest"*. The *"use of CNE to weaken software or hardware at its source, prior to its deployment to users"*, and *"the obtaining of information for the purpose of maintaining or further developing the intelligence services' CNE capabilities"* were also alleged but *"neither confirmed nor denied"* by the GCHQ.[1154] The GCHQ carried out CNE *"within and outside the UK"* and, in 2013, *"about 20% of GCHQ's intelligence reports contained information derived from CNE"*.[1155] These practices appear to be still active and are also covered by the new investigation framework[1156].

Other administrative authorities

In relation to other public administrations, some questionable practices have also been reported. They globally appear to show a lack of transparency, of minimisation or of other privacy guarantees.

For example, the creation of a health data base in order to support the fight against the pandemic, called the *"Covid-19 datastore"*, has been challenged for not protecting personal data appropriately[1157]. In particular, criticism highlighted the opacity surrounding operations and the choice of controversial subcontractors such as Palentir.[1158]

It is also noteworthy that on 9 May 2019, the UK Data Protection Authority (ICO) issued an enforcement notice against the Her Majesty Revenue & Customs (HRMC) which is *"the tax, payments and customs authority of the United Kingdom"*[1159]. The ICO established that starting in January 2017, the HRMC collected the voice of its 7 million customers in order to obtain a voice-ID as future means of authentication. However, this biometric identifier was collected without informed consent from the persons concerned.[1160] Consequently, based on the GDPR,

the ICO required the deletion of *"all of the biometric data held under the Voice ID system for which [the HRMC did] not have explicit consent"*[1161].

B. PRIVATE USAGE OF SURVEILLANCE TECHNOLOGIES

Private video-surveillance is massive. In 2008, the CCTV User Group addressed the use of CCTV by multiple stakeholders such as *"Universities, Major Shopping Malls, Hospitals, Ports and Airports, Train and Bus Stations, Retail and Commercial Users"*[1162]. In 2019, BBC News noted that the *"manufacturing of CCTV cameras and facial recognition technologies is a booming industry, feeding a seemingly insatiable appetite"*[1163].

The use of biometric surveillance is also reported as widely used in the construction industry[1164]. In 2015, a report showed that *"25% of UK retailers are using facial recognition technology in an effort to monitor customer activities at their stores"*[1165]. In 2017, the first supermarket to enable payments using hand veins was reported[1166]. The NatWesk banking group announces they are developing behavioural biometrics technology which could replace banking passwords[1167].

In addition, several educational institutions use fingerprints in order to handle absenteeism, to charge meals, and as a substitute for library cards. It led to some contests and new legislation imposed parents' consent 1168. From this date forward other practices of the same kind have been reported. For example, the cafeterias of nine British schools in the North Ayrshire are to implement facial recognition for payment. It is reported that a lot of parents approved, but there were also contestations. For example, the UK Biometrics Commissioner considers that *"facial recognition is arbitrary"* and fears *"that the installation in schools will educate children and young people to accept restrictions on data protection"*.[1169]

3) POLITICAL STANDING IN RELATION TO THE USE OF MASS SURVEILLANCE TECHNOLOGIES

Governmental practices tend to show a will to massively use surveillance technology under the justification of security and progress.

Edgar A Whitley and Gus Hosein report that, during debates that surrounded the adoption of the 2006 Identity Cards Act, *"progress"* was *"the prevailing discourse"* presented to the media".[1170] *Other public representatives evoked the idea of "*civilisation*"*[1171]*, and the need to fight terrorism*[1172]*. In this context, Whitley and Hosein report that the London School of Economics and Political Science (LSE) issued a* 300-*page report highlighting a series of concerns posed by the identity scheme. These concerns include the lack of precise and demonstrated purpose, suggesting that the scheme had been "*gold-plated*"* to justify its need.[1173] Amongst other concerns were the cost of the scheme, the lack of operational efficiency, the lack of privacy and security assessments, and the lack of study relating to citizens acceptance and business benefit.[1174]

Whereas the intention behind the LSE work *"was to enhance the policy debate"*[1175], Whitley and Hosein explain that the government attacked the integrity of the LSE and of the researchers themselves, and that the Home Office used *"bullying and intimidation"* against them.[1176] This ended in 2006 with the adoption of the text, as its implementation *"faced a number of problems almost immediately"* and the researchers were *"being called upon to provide independent analysis"*.[1177]

In 2005, The Register reported that the UK was *"using its Presidency of the Council of the European Union to push for the adoption of biometric ID cards and associated standards across the whole of the EU"*.[1178] Moreover, the decisions from the Investigatory Powers Tribunal show that intelligence services use intrusive surveillance for decades, in opacity when they are not required to report it.[1179] We also note a certain tendency, for public authorities, to modify laws in order to make them cover practices, instead of modifying such practices, where the latter are found to be disproportionate.

The area of live facial recognition illustrates this perfectly. In 2012, a high court ruled *"that keeping images of innocent people"* in biometric databases *"was unlawful"*[1180], but it appears that *"police forces have quietly continued to build up a massive database without any of the controls or privacy safeguards that apply to police DNA and fingerprint databases"*. The Home Office said that the deletion of the images of *"people who were not convicted of an offence"* would be *"extremely lengthy and resource intensive"* because *"the police national database does not link custody images to individual crime records"*.[1181] In this context, the Home Office is accused, by the ONG Liberty, of *"knowingly breaching the law for years"*. This organisation specifies that *"police hold thousands of pictures of activists and bystanders who were never even taken into custody and may not know their photo was taken"*.[1182] In 2017, 19 million images were inventoried in the database, and the Commissioner for the retention and use of biometric material observed that the *"somewhat anarchic situation"*, in terms of facial images governance and standards, *"runs the risk of false intelligence or wrongful allegations"*[1183]. Nevertheless, in 2018, the government published a biometric strategy, which provides LEAs with *"greater powers to use biometric technology on the street"*[1184]. The strategy also intends to enhance data governance, ethics, privacy by design and oversight, in a chapter entitled *"Maintaining Public Trust"*.[1185] In 2020, despite criticisms, the London Metropolitan Police announced the deployment of facial recognition in the streets. A few months later, such use was declared contrary to the ECHR by a Court of Appeal, in a decision targeting South Wales police practices[1186]. However, in August 2021, the government opened to consultation, for a period of four weeks, a revised version of the Surveillance Camera Code of Practice[1187], which constitutes one of the legal texts to be respected by law enforcement. This revised version includes the possibility for LEAs to use facial recognition. Several NGO are currently *"accusing the UK Home Office and police of bypassing Parliament to*

introduce live facial recognition technology".[1188] They especially argue that the guidance was released *"during the parliamentary summer recess [...] without any publicity or official announcement"*. They *"call on members of parliament and peers to demand a full parliamentary debate on the use of LFRT"*.[1189]

7.2.2. LEGISLATION REGULATING MASS SURVEILLANCE TECHNOLOGIES

The United Kingdom does not have a written Constitution, for historical reasons. Democracy *"is based on Acts of Parliament, historical documents, court judgments, legal precedence and convention"*.[1190] Human rights are guaranteed by the Human Rights Act of 1998, which gives *"further effect to rights and freedoms guaranteed under the European Convention on Human Rights"*[1191]. As a result, the Act guarantees the rights enshrined in articles 2 to 12 and 14 of the European Convention on Human Rights.[1192] In particular, Schedule 1 Part 1 of the Act guarantees the right to life (art. 2), the prohibition of torture (art. 3), the right to liberty and security (art. 5), the right to a fair trial (art. 6), the principle of no punishment without law (art. 7), the right to respect for private and family life (art. 8), the freedom of thought, conscience and religion (art. 9), the freedom of expression (art. 10), the freedom of assembly and association (art. 11), the prohibition of discrimination (art. 14) and the right to education (part II of the First Protocol, art. 2). In addition, judges have the duty, within their rulings, to take into account the decisions of the EctHR and of the Council of Europe Committee of Ministers[1193].

The General Data Protection Regulation (GDPR) and Directive 2016/680, which applies to judicial and police data processing, were implemented in the Data Protection Act 2018[1194]. The United Kingdom authority, named ICO, enforces their respect.[1195]

Part III of the Act regulates law enforcement activities. According to the ICO, the use of facial recognition by law enforcement authorities is subject to the application of these provisions[1196]. Part IV of the Data Protection Act 2018 regulates the activities of the three UK intelligence services: MI5, MI6, and the GCHQ[1197]. However, most provisions of Part IV do not apply where an exemption *"is required for the purpose of safeguarding national security"* (Part IV, article 110). In this case, a Minister of the Crown may issue a certificate certifying that the exemption is or was required. Any person directly affected by the issuing of a certificate may appeal to the Tribunal against the certificate (art. 111). Such certificate *"is conclusive evidence"* of the fact that the exemption was required (art. 111). The same rule applies in relation to law enforcement activities regulated under Part III (art. 79). As it was highlighted by a NGO, this procedure leads to opacity in relation to national security activities, and is *"open to abuse"*[1198].

In addition, several laws base the missions and powers of the MI5 (the Security Service Act 1989[1199]) and of the MI6 and GCHQ (Intelligence Services Act 1994[1200]). Their powers of investigation are framed by the Regulation of Investigatory Powers Act 2000[1201], which has been implemented through several Codes of Conduct[1202] in the areas of gathering Communications Data[1203], Interception of Communications[1204], Covert Surveillance[1205], use of Covert Human Intelligence Sources[1206], Equipment Interference[1207] and Bulk Data[1208]. A surveillance Camera Code of Practice[1209] is also under modification[1210].

This legislation has been updated by the Investigatory Powers Act 20161211, which is criticised because intelligence and police services with extended powers that are deemed to be disproportionate[1212].

Moreover, intelligence and police services are subject to other specific legislation such as the Terrorism Act 2000[1213], the Anti-Terrorism, the Crime and Security Act 2001[1214], the Terrorism Act 2006[1215], the Counter-Terrorism Act 2008[1216] and the Terrorism Prevention and Investigation Measures (TPIMs) Act 2011[1217].

In relation to facial recognition, in the context of a lack of dedicated legislation, the Metropolitan Police publishes a set of guidances[1218].

Overall, the legislation provides a wide range of safeguards. In particular, it ensures a relative transparency of the existence of powers and of the requirements of legitimate purpose, efficiency and minimisation. Intelligence services are also acting under the supervision of the Investigatory Powers Commissioner's Office (IPCO)[1219].

However, there is no certainty that the principles that are established are, in practice, properly implemented and supervised. Indeed, enforcement and supervision mechanisms appear to remain weak. This can be illustrated by a 2020 report from the UK Surveillance Camera Commissioner. It established that only 50% of local authorities responded to a survey on their compliance with the Code, and that many respondents declared that they had not so far considered being certified in relation to such compliance because *"their processes and procedures"* needed to get improved. Overall, this means that transparency is not really ensured towards all video-surveillance systems, in particular in relation to their purposes[1220], and that supervision appear widely of a declarative nature.

7.2.3. CIVIL SOCIETY RESPONSES

Several NGOs are active in the United Kingdom, in particular Privacy International[1221], Liberties[1222], and Statewatch[1223]. They regularly inform the population about the public measures they deem disproportionate and challenge them before courts, often successfully[1224].

The press is also very active in informing citizens. Several newspapers give great importance to surveillance issues, such as The Guardian, The Telegraph, Breitbart and the BBC.

According to a report from the House of Commons Science and Technology Committee (HCSTC), Citizens and residents seem highly concerned *"about intrusions into both their 'physical privacy' and their 'informational privacy'"*[1225]. Professor van Zoonen considers that public anxiety is *"centred on at least three areas: first, 'strong cultural associations' of biometrics with 'state control and surveillance'; second, fears about losing control over personal data, with data subsequently being 'lost or abused'; and third, concerns about whether personal data was acquired and stored securely"*[1226].

The HCSTC explains that *"this absence of public 'faith and trust'*[1227] *was highlighted as a key challenge facing both the Government and industry, and a "*primary inhibitor*" to the development and implementation of biometric systems"*.[1228] The Committee observes that the government *"appears to have made little effort to engage with the public regarding the increasing use of their biometric data"*[1229] and that *"recent 'breaches of security', including the 'Snowden incident', have made the public increasingly sceptical about who has access to their biometric data and whether it is stored securely"*[1230]. This, in a situation where *"the theft of an individual's biometrics [creates] a 'security nightmare' whereby somebody's biometrics [are] 'no longer available to them to authenticate themselves for the rest of their lives'"*[1231].

As a result, public opposition has slowed down the implementation of biometry. Public opposition is also partly responsible for the scrapping of the identity scheme in 2010. Indeed, Edgar A. Whitley and Gus Hosein explain that, during debates surrounding the adoption of the Identity Cards Act 2006, a new NGO was created to fight the policy, called NO2ID. The authors report that *"in the ensuing years it became significantly larger with greater resources to provide briefings to parliamentarians. Other human rights groups also emerged as opponents to the Scheme and these groups played a significant part in raising public and political interest in the issue"*.[1232]

7.3 ROMANIA

7.3.1. STATE OF USE OF SURVEILLANCE TECHNOLOGIES

1) CURRENT OFFLINE USE, BY PUBLIC AUTHORITIES, OF BIOMETRIC AND BEHAVIOURAL MASS SURVEILLANCE TECHNOLOGIES

Identity documents

Romania implemented passports with fingerprints, the latter being stored in a chip in the passport and not collected in a database[1233]. In August 2021, biometric ID cards started being issued.[1234] They include two fingerprints and a photograph, in addition to the national identity number (CNP), but a possibility to refuse biometry is available, leading to the delivery of a regular ID card instead[1235]. Beyond its aim to ease the exercise of free movement[1236], this new ID card is planned to be used as a *"health card, through a digital certificate inscribed on its chip"*, to enable access to *"various electronic services (banking, fiscal, social, financial, and educational) and, make use of the electronic signature based on a certificate"*[1237]. However, details remain unclear.

The EU Regulation on strengthening the security of identity cards[1238] make it mandatory to destroy biometric identifiers after the biometric ID card has been issued, unless other necessary and proportionate processing would be decided at national level in accordance with Union and national law. However, it is alleged that Romanian public authorities maintain a *"facial recognition database with some 50-60 million facial images (such as ID cards or passports), to which the Romanian Intelligence Service (SRI) has unlimited and unsupervised access"*[1239], without specific legislation providing for it. However, this has not been confirmed and therefore remains only speculation.

Romania is also involved in the Schengen Information System (SIS II), which includes fingerprint, palm print, and facial image[1240], and belongs to the half-group of States that provide information leaflets on SIS II, following the EU campaign that aims to ensure transparency towards potential data subjects[1241]. Romanian access to the Automatic Fingerprint Identification System (AFIS)[1242] appears to be regulated in compliance with the EU requirements in that field.

In 2012, a project co-funded by Romania and Switzerland drove to the implementation of a *"cutting-edge laboratory equipment for fingerprint recovery from various supports and in atypical conditions"*, which enabled an upgrade of Romania's Automatic Fingerprint Identification System (AFIS). AFIS can be accessed by Romanian police forces in the country as well as border police inspectorates for European cooperation purposes, the system being further *"interfaced with the European databases for automatic data exchange"*.[1243]

Video-surveillance

In relation to video surveillance, it is difficult to evaluate the overall number of cameras implemented in Romania. However, even though it appears to be lower than in other countries such as France or the United Kingdom[1244], several cities declare using video surveillance in order to discourage illegal acts. An example is one district of Bucharest, which possessed at least 375 surveillance cameras in 2019 with the aim of sending fines to persons whose cars were caught to be at the scene of illegal waste dumping[1245]. Another example is the case of Slatina, a city located in the south of Romania, which implemented a video-surveillance system in order to prevent crime. This system is *"based on 150 AXIS 233D Network Dome Cameras, 200 infrared illuminators and 150 outdoor speakers installed on 150 metal poles with climbing deterrents all connected to a dispatcher located in Slatina City Hall"*[1246]. Its provider is a company founded in Latvia and present in 11 countries.[1247]

In addition, a recent study highlights an increasing use of CCTV including facial recognition in the country, in association with biometric databases[1248].

However, limited information is provided in relation to this phenomenon, beyond some rare media articles.

The General Inspectorate for the Romanian Police has also decided to equip law enforcement with 12,000 body-worn cameras, purchased from the American company Motorola. These cameras enable the full recording of scenes and live streaming to a control room. The purpose declared is to improve the safety of both the police and the public, to enhance the accountability of forces and to enable the production of evidence before court in case a police intervention would be challenged.[1249] At this stage, there is no schedule to use these cameras for biometric surveillance purposes, but the Motorola model allows the possibility to send live images that could technically be monitored using biometric or behavioural recognition systems, directly or in a second phase. The Romanian Border Police also invested in more than 3,000 cameras of the same kind some months afterwards[1250]. These decisions followed a pilot project that started in 2017.[1251]

Additionally, a National Biometric Identification System (NBIS) became operational in 2016. It contains information, including facial images, of people targeted by the Romanian Police, such as missing people, unidentified people, suspects, criminals, and unidentified bodies. In 2019, the Romanian Police launched a public procurement for acquiring facial recognition and training solutions.[1252] The aim was to enable comparing the NBIS database with digital facial images coming from different sources, such as CCTV, webcam, mobile phones, and ATM cameras.[1253] The Romanian Police declared that the system aims to identify people under investigation and that it does not include live recognition features. It specified that the system does not include technical specifications that enable monitoring and storing of information from private and public spaces.[1254] However, an annex to the technical specifications list includes automated facial recognition capabilities for comparing and verifying images of unidentified people with digital images from the facial images database.[1255] The company which was awarded the project is called Dataware Consulting and other companies who applied for the close to EUR 1 million contract are Tech Source Consulting with Cymbiot Solutions and Avatar Software as subcontractors, Starc4sys SRL, RECO and Idemia Identity&Security France.[1256] Several NGOs raised concerns about this project and wrote an open letter to the Ministry of Internal Affairs, the Romanian Data Protection Authority, the Ombudsman and the Chamber of Deputies. They highlighted the lack of prior consultation with the Romanian Data Protection Authority and civil society. They also pointed out a series of concerns including the lack of any impact assessment and of any clarification on how peoples' rights to privacy will be protected and guaranteed. They specified that no information was available in relation to security measures, privacy safeguards, and transparency measures.[1257] Amongst their demands, the four NGOs asked for the public procurement to be annulled.

Other biometric and behavioural recognition experiments

In 2013, the Bucharest airport was used to test a system named Automated Virtual Agent for Truth Assessment in Real time (AVATAR), developed by the US National Centre for Border Security and Immigration. It enabled the conducting of automated interviews of travellers associated with the analysis of the latter's *"nonverbal and verbal behaviour, such as eye movement, gestures and pitch"*.[1258] In 2019 operations began to expand and modernise the same airport's video surveillance system, to be completed in 2023. Modernisation includes the implementation of features such as automatic recognition of cars' registration numbers, facial recognition and intelligent video analysis. Operations are implemented by the UTI Group, a Romanian company.[1259]

The start of the cooperation between UTI and the Bucharest airport dates back to 1997 whereas other partnerships were concluded during the following years, for example with the Underground Transportation Company (automated fare collection solution), the Ministry of Defence (command and control system) and some Romanian cities (complex traffic management system). UTI also exports surveillance systems abroad such as in Yemen.[1260]

Finally, it must be mentioned that Romania's Border Police uses unmanned aerial vehicle (UAV), provided by the European stakeholder Nordic Unmanned[1261]. This technology is used *"for multipurpose coast guard missions over the Black Sea, which include maritime pollution monitoring, detection of illegal fishing, border surveillance and search and rescue operations"*. The data collected during drone flights are *"transmitted in real time to users via the European Maritime Safety Agency (EMSA)'s Remotely Piloted Aircraft System (RPAS) Data Centre"*, through a satellite communication.[1262]

2) OTHER USAGES OF SURVEILLANCE TECHNOLOGIES

A. PUBLIC USAGE OF SURVEILLANCE TECHNOLOGIES

In Romania, each citizen has a National Identification Number called Numerical Personal Code (CNP).[1263] This code is indicated on new biometric identification cards.

In 2019, the Romanian Intelligence Service (SRI) completed the implementation of a project called *"SII ANALYTICS - Information system for the integration and operational and analytical exploitation of large volumes of data"*, co-funded by the European Regional Development Fund through the Competitiveness Operational Programme 2014-2020.[1264] In 2016, four organisations expressed concerns in relation to this project, due to its *"potential for widespread surveillance of the entire population of Romania"*[1265]. Complaints were sent to the European Commission, the European Anti-fraud Office (OLAF), the Romanian Data Protection Authority, and the Parliamentary Committee overseeing SRI's activity. Answers received from these authorities did not clearly address the main concerns.[1266] The SRI declared that, in its opinion, SII Analytics does not threaten citizens' rights and freedoms[1267]. It clarified that new developments only aimed to modernise the Romanian data processing system by using algorithms, in order to exploit existing data more efficiently. It specified that no connection to the internet and no collection of new personal data were foreseen, and that access control and filters are implemented to identify any unauthorised use of the system.[1268] Nevertheless, several questions remain unanswered, which maintains a lack of transparency. These questions especially relate to the identification of the legal basis that frames such a data processing system, to the sources of the information that is aggregated, to the services that access this system[1269], and to conditions for access (over 750 terminals being likely to have access to it). Questions also relate to the setting up of guarantees against arbitrary access in light of verbal statements that *"every query will be automatically logged and analysed to avoid abuses"*[1270]. In this respect, there is a fear that a *"behavioural file"* is established in order to enable a *"behavioural analysis"* that would be included as a feature of the system.[1271]

Service providers involved in the development of SII Analytics appear to be Siveco, Nova Tech, BAE Systems as well as the Romanian company Romsoft International.[1272] The SII Analytics project was built on SII Infrastructure which was implemented by Logika IT Solutions, Datanet Systems and Siveco Romania (through Logic Computer as subcontractor) for data centers, and by Datanet Systems and Mira Telecom for broadband.[1273] It is reported that the SII Infrastructure project, created in 2003, operates based on a decision of the Romanian Supreme Council of National Defence (CSAT) which is not publicly available. Some voices deplore this lack of transparency and report that the CSAT decision was issued at the request of the head of the SRI Alexandru-Radu Timofte, who described the SII as *"a huge IT machine containing data and information stored on the basis of protocols with 11 or 21 state institutions"*[1274]. Some months after the publication of Law 161/2003 on anticorruption (implementing Title III the Cybercrime Convention), the government issued a government decision to operationalise the SII. This decision was unsuccessfully contested in court by the Romanian Human Rights Organisation APADOR-CH.[1275]

B. PRIVATE USAGE OF SURVEILLANCE TECHNOLOGIES

Several private stakeholders use intelligent video-surveillance solutions. In particular, the Russian solution called TRASSIR is distributed by the Romanian companies Romanian Security Systems SRL (RSS)[1276] and Azitrend[1277] within the framework of their own security services. TRASSIR for example is used by Auchan hypermarkets in Romania, where it provides access to control systems, burglary systems, anti-theft detection gates, fire safety systems, video analytics able to monitor all POS transactions in order to *"prevent any fraudulent activity and detect human errors"*: in case of any suspicious situation, *"ActivePOS immediately sends automatic notifications to the operator"*.[1278] TRASSIR is also in use in another supermarket chain[1279], a major supplier of agricultural products (450 video channels spread into 15 locations)[1280] and a major supplier of construction materials[1281]. This supplier uses a TRASSIR function called 'Neuro Detector*", which can notably detect human presence and map people movements (people from the staff may be excluded using specific clothes colours)*[1282]*. Based on "*neural networks of deep learning*", this solution is considered by its provider as an offline equivalent*

*of Google Analytics since it measures "*metrics that directly affect the traffic and conversions in offline business*"*[1283].

Beside this, a Romanian start-up proposes a *"fully automated Know-Your-Customer (KYC) solution"* which enables providers to identify their customer through comparison between their biometric identity card and the facial recognition of their face through their webcam[1284]. The proposed solutions declares to appropriately protect personal data during *"collection, processing and storage"*[1285] without clarifying the retention length, destruction conditions, and recipients of collected data. Other examples of start-up initiatives include the Romanian fintech PayByFace. It developed a facial recognition-based payment system which may be used in any partner store as an alternative to other means of payment[1286]. In 2020, businesses such as meal and gift card issuers[1287] and Romanian coffee shops[1288] introduced the biometric facial recognition-based payments system. In 2021, Raiffeisen Bulgaria piloted a project with PayByFace in order to *"introduce an easier, more attractive, and more secure way of payments for their clients"*.[1289]

3) POLITICAL STANDING IN RELATION TO THE USE OF MASS SURVEILLANCE TECHNOLOGIES

Romanian authorities express a strong wish to strengthen the Romanian national security[1290], which is understood in a wide approach that links *"all dimensions"* including, non-exhaustively, political, civic and societal ones[1291]. Defence spending over the period 2001-2017 increased substantially, as well as the *"ratio allocated for equipment expenditures"* which rose by more than 50% from 2016 to 2017, to represent roughly one quarter of the total expenditure[1292]. Research and development in the field seems ongoing[1293], while public-private partnerships are seen in a favourable light[1294]. Implementation of surveillance technologies generally relies on a provider, a large part of them appearing to be located in the European geographic zone.

Combined with current practices in the field[1295] (see previous subsections of the current study), the willingness assigned to the political class to evolve towards more control[1296] is plausible, especially through the action of state intelligence services (SRI). Indeed, whereas SRI seems to be internationally considered as capable of efficiently monitoring individuals[1297], whether their intent is known or unknown, and whereas these services are perceived to be tempted by ideas about exerting *"extensive control over the population»* in addition to *«silencing its critical intellectuals»*[1298], some questions have been raised more recently in relation to separation of powers in the country[1299] and to non-enforcement of court decisions against the State[1300], as well as in relation to a continuous tendency to attempt to implement more non-biometric surveillance measures.

For example, from 2011 onward, there have been six attempts to impose mandatory SIM cards registration. The most recent one, introduced by Emergency Ordinance in September 2019, was declared unconstitutional by the Romanian Constitutional Court on 18 February 2020.[1301] The fourth attempt was contemporaneous with the Snowden revelations.

Shortly after the Snowden revelation, in July 2013, a controversial public representative, member of the joint permanent commission of the Chamber of Deputies and the Senate for the exercise of parliamentary control over the activities of the SRI, declared that the aim of the legislative authority was to enable the interception of *"pre-paid phone cards by the secret services"*, being *"in favour of the implementation of a PRISM programme in Romania, which would allow the surveillance of communications on the Internet, in case of suspicions of terrorism or serious economic crimes, arguing in the face of criticism that often the protection of private life is invoked 'but the desire is to defend freedom to crime'»*. He also expressed the will for the secret service to gain the ability to intercept all the electronic means of communication as well as access the history of peoples' activities[1302]. Other political representatives exposed views of the same nature, the political being considered as seeing *"in mass surveillance not a problem but a desirable goal to be attained with no consideration for what the public wants"*[1303]. After the CJEU declared the Data Retention Directive invalid, the Romanian government decided to maintain in force Law 82/2012 which enables data retention (it was adopted despite persistent criticism[1304], after invalidation of the previous data retention law by the Romanian Constitutional Court in 2009[1305]). In 2014, the Romanian parliament adopted a new law on security, granting several public authorities, including the SRI, the power to search computer systems without a court order. The Constitutional Court ruled this cybersecurity law unconstitutional.[1306]

The National Institute for Research and Development in Informatics (ICI) Bucharest is currently involved in a public service digital identity project in partnership with the Romania-based digital identity firm selfd. id[1307], aiming at accelerating *"the digitisation of the national public system in the country"* by enabling *"individuals' interaction with government institutions"* through a *"decentralised digital identity platform"* and the *"creation and adoption of a secure electronic public identification (e-ID) system"*[1308] aligned with European requirements[1309].

7.3.2 LEGISLATION REGULATING MASS SURVEILLANCE TECHNOLOGIES

The Romanian Constitution guarantees a series of fundamental human rights, including equality of rights (art. 16), right to defence (art. 24), freedom of movement (art. 25), personal family and private life, inviolability of the domicile and the secrecy of correspondence (arts. 26-28), freedom of conscience (art.20), freedom of expression and the right to information (arts. 30 and 31), right to education (art. 32), and freedom of assembly and of association (arts. 39 and 40). Some of these rights are also penally protected and enforced in the penal procedure Code, which for instance states that the prosecutor must inform in writing the subject of a surveillance measures, once the latter has ended. Surveillance during investigations appears to be framed and can only be decided based on reasonable suspicions.[1310]

In addition, Romania adhered to the European Convention on Human Rights, which came into force in June 1994[1311]. This Convention prevails on the Constitution in case of inconsistency, *"unless the Constitution or domestic laws comprise more favourable provisions"*, according to article 20 of the Constitution. Following the ECHR principles, article 53 of the Constitution establishes that the exercise of freedoms may only be restricted by law for a list of limited purposes amongst which lies the defence of national security, provided that restrictions are necessary in a democratic society and proportionate.

Moreover, the Constitutional Court seems to be vigilant in the field of fundamental rights protection. It declared unconstitutional several laws that were criticised for their unnecessary and/or disproportionate nature, such as the first data retention law[1312] and successive laws aiming at making identification mandatory to use pre-paid SIM cards[1313], as well as the first cybersecurity law[1314].

The General Data Protection Regulation (GDPR) was implemented in law n° 190/2018[1315]. Directive 2016/680, which applies to judicial and police data processing, was transposed into law 363/2018[1316]. The Romanian supervisory authority, called ANSPDCP, has some activity in the field of private use of biometric and video surveillance[1317] and has issued guiding decisions[1318]. In its answer to the SII Analytics complaint, the ANSPDCP especially clarified that Romanian public authorities without national security attributions are subject to the application of law 677/2001 (which implemented Directive 95/46/EC on the protection of personal data before it was replaced by law 190/2018).[1319]

In relation to SRI activities, the ANSPDCP considers that they are exempted from the application of Law 190/2018, because their tasks are a matter of national security. The data protection authority also noted that the legal basis for data processing replicating databases, including within the framework of the SII Analytics system[1320], is the Government Ordinance 952/2003[1321].

For the rest, the SRI is coordinated by the Supreme Council for National Defence (CSAT). Its activities are regulated by law n° 51/1991 on national security[1322] and by law n° 14/1992 on SRI's functioning. It is moreover subject to law n° 535/2004 against terrorism, to law n° 544/2001 on access to public information and to law n° 182/2002 on classified information.

Despite the existence of such regulations, several voices deplore a huge lack of transparency of the SRI activities.[1323] In particular, it remains unclear whether the SRI is using biometric recognition technology under the SII Analytics and how it is regulated. In addition, there is no information available in relation to the SRI powers in terms of access to other databases, whether of a public (including criminal) or a private nature. Article 13 of law n° 51/91 only regulates the access, by intelligence services, to other databases and information through search and seizure, by request to the public prosecutor and in compliance with the penal procedure Code. It is

to be noted, on this aspect, that subsequent usages of collected information and the length of their retention are not particularly clarified. For the rest, SRI's activities are covered by state secret, whose definition is considered to be *"vague"*[1324].

Moreover, the control over the SRI's powers seems insufficient. It only relies on a parliamentary control, whose modalities are also not clarified (article 9 of law n° 51/91). In this regards, it is worth noticing that, in 2014, a member of the joint permanent commission for the exercise of this parliamentary control expressed the will that the secret service gain the ability to access the history of peoples' activities, declaring that the defence of private life often reveals the desire *"to defend freedom to crime»*[1325].

In relation to SII analytics particularly, we can also note that government ordinance 952/2003 does not appear to regulate the new developments of the system. Consequently, a specific legal basis would be required based on the ECHR requirements[1326]. In its absence, the legal framework does not appear to provide for sufficient safeguards[1327]. At the minimum, clarifications would be needed concerning the entities and persons who can access the database[1328], the purposes and the situations in which such access may be granted, the extent of their powers in terms of data reproduction and retention period, the conditions under which databases interconnections may be allowed, the nature of the data involved and the mechanisms that ensure effective control over these powers.

It is worth noting, on this particular issue of the exchange of data between public authorities, that the CJEU ruled, in 2015, that the Romanian Tax Authority (ANAF) could not, *"on the basis of a single internal protocol"*[1329], transfer data to another public authority *"for purposes other than those for which [these data] had initially been communicated to the ANAF"*, without prior explicit and informed consent of the person concerned.[1330]

7.3.3 CIVIL SOCIETY RESPONSES

Beyond reactions from civil society organisations[1331] and dissemination of information from legal specialists[1332], some modest citizens-based protest movements have been noticed[1333]. However, most Romanian people do not seem to strongly react to questionable legislative proposals or practices connected to biometrics and surveillance.

This might be firstly explained by the fact that terrorism and immigration – two issues that are often used to justify restrictions of freedoms - were not part of major concerns of the public opinion in studies conducted in 2004 and 2017, contrary to the tendency that was noticed in other EU countries[1334].

Among other reasons for this apparent lack of interest lies an apparent lack of effective information regarding the European Union[1335] and political agendas more generally. In addition, *"a large percentage of the population [lives] in rural areas"*[1336], where people may encounter *"unemployment and poverty"* issues[1337] and a *"lack of affordable and easy access to the internet"*[1338].

The lack of reaction on the part of citizens toward questionable public measures also appear to come from a feeling of hopelessness and disbelief that one or more individuals can realistically change anything. This is induced by the *«no big deal»* attitude of public authorities, generally accompanied by an attitude of *"no consideration for what the public wants"*, as it was pointed out by a member of ApTI, a Romanian digital rights NGO. The author considers that the attitude of public authorities, where they silence debates and then reiterate their proposal despite Constitutional Court negative decisions, makes most Romanians *"internali[sing] the situation and fall[ing] back into their default state of resignation, gallows humour or a combination of the two, with no actual conversation having taken place between civil society, weak as it is"*.[1339]

974. These documents are listed in Decree n°2007-255 of 27 February 2007 (modified by Decree n° 2014-512 of 20 May 2014), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000614884.

975. Decree n°2008-426 of 30 April 2008 modifying decree n°2005-1726 of 30 December 2005 "relatif aux passeports électroniques", JORF, n°0105, 4 May 2008, https://www.legifrance.gouv.fr/jorf/id/JORFARTI000018743968; Thierry Plette-Coudol, 'Données publiques. Production interne et collecte sur le secteur privé', 4 mai 2020, JCL Adm., LexisNexis, Fasc. 109-40, p. 74.

976. Biometric identity card is delivered from the 2 August 2021: Alice Vitard, 'Trois questions sur la nouvelle carte d'identité biométrique', 3 August 2021, https://www.usine-digitale.fr/article/trois-questions-sur-la-nouvelle-carte-d-identite-biometrique.N1130609; Decree n° 2021-279 of 13 March 2021 "portant diverses dispositions relatives à la carte nationale d'identité et au traitement de données à caractère personnel dénommé 'titres électroniques sécurisés' (TES)", https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043246707 ; https://www.cnil.fr/fr/le-fichier-des-titres-electroniques-securises-tes.

977. Decree n°2012-497 of 16 April 2012 "relatif au recueil des images numérisées du visage dans certaines communes des départements et collectivités d'outre-mer et des empreintes digitales des demandeurs de passeport", JORF, n°0092, 18 April 2012, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000025705936/; Christiane Feral-Schuhl, 'Cyberdroit. Le droit à l'épreuve de l'internet 2020/2021', Dalloz, 8th ed., 2020, p. 359.

978. Decree n°2016-1460 of 28 April 2016 "autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité", article 10, JORF, 30 October 2016, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033318345/2021-11-21/.

979. Created by Decree n°2016-1460 of 28 April 2016, already mentioned.

980. Article 2 of Decree n°2016-1460 of 28 April 2016, already mentioned.

981. Article 9 of Decree n°2016-1460 of 28 April 2016, already mentioned.

982. Regulation (EU) 2019/1157 of 20 June 2019 on strengthening the security of identity cards, article 10, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1157.

983. Article 1 of Decree n°2016-1460 of 28 avril 2016, already mentioned.

984. Article 4 of the decree n° 2016-1460 of 28 October 2016, already mentioned. See also Article L122-1 of the Internal Security Code, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042919869/.

985. Decree n° 2021-279 of 13 March 2021 "portant diverses dispositions relatives à la carte nationale d'identité et au traitement de données à caractère personnel dénommé « titres électroniques sécurisés"(TES), Article 10, JORF n°0063 of 14 March 2021, https://www.legifrance.gouv.fr/jorf/id/JORFARTI000043246719.

986. See our discussion in subsection 7.1.1.3 of the current study.

987. See subsection 7.1.2 of the current study.

988. See subsection 7.2.1.2.1 of the current study.

989. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 22, https://hal.archives-ouvertes.fr/tel-02439529.

990. Translated from French: Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, already mentioned, p. 55.

991. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, already mentioned, p. 51. See also Ministère de l'Intérieur, Videoprotection, 'Le guide méthodologique', https://www.interieur.gouv.fr/Videoprotection/Le-guide-methodologique.

992. Paul Bischoff, 'Surveillance camera statistics: which cities have the most CCTV cameras?', 17 May 2021, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/. See also Ma Forteresse, 'Vidéosurveillance : Histoire de la caméra de surveillance', https://www.maforteresse.com/guide/videosurveillance-histoire-de-la-camera-de-surveillance.html#Quelques_chiffres_sur_lutilisation_actuelle_de_la_camera_de_surveillance, which evokes a ratio of 68,4 cameras for 1,000 inhabitants.

993. Translated from French: Rédaction, 'Quand la France se lance dans la reconnaissance faciale', 2 October 2019, Next INpact, https://www.nextinpact.com/article/29687/108256-quand-france-se-lance-dans-reconnaissance-faciale.

994. See the thematic dossier on Biometrics on the CNIL's website: https://www.cnil.fr/fr/biometrie. For an overview of cameras and technologies implemented in different French cities, see the map proposed by the movement "Technopolice" at https://technopolice.fr/villes/.

995. Stephen Mayhew, French National Police using Safran's Morpho Video Investigator solution, 1 December 2016, BiometricUpdate.com, https://www.biometricupdate.com/201612/french-national-police-using-safrans-morpho-video-investigator-solution.

996. Martin Untersinger, 'La reconnaissance faciale progresse, sous la pression des industriels et des forces de l'ordre', 14 October 2019, Le Monde, https://www.lemonde.fr/pixels/article/2019/10/14/sous-la-pression-des-industriels-et-des-

forces-de-l-ordre-la-reconnaissance-faciale-progresse_6015370_4408996.html.

997. Ryan Mac, Caroline Haskins and Antonio Pequeño IV, 'Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here', 25 August 2021, BuzzFeed News, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

998. Translated from French: Ryan Mac, Caroline Haskins and Antonio Pequeño IV, 'Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here', already mentioned.

999. See articles 230-6 s. of the penal procedure Code, https://www.legifrance.gouv.fr/codes/id/LEGISCTA000023709609.

1000. Pierre Januel, 'Police : l'utilisation massive de la reconnaissance faciale se confirme', 19 October 2020, Next INpact, https://www.nextinpact.com/article/44242/police-utilisation-massive-reconnaissance-faciale-se-confirme#/page/2. The author refers to a report presented to the National Assembly and to debates that took place before this same assembly.

1001. 20 Minutes with AFP, 'Commande de 30.000 caméras-piétons pour équiper les policiers français', 6 May 2021, 20 Minutes, https://www.20minutes.fr/societe/3036631-20210506-commande-30000-cameras-pietons-equiper-policiers-francais.

1002. AFP, 'Police: généralisation des caméras-piétons au 1er juillet 2021', 14 September 2020, Le Point, https://www.lepoint.fr/societe/police-generalisation-des-cameras-pietons-au-1er-juillet-2021--14-09-2020-2391720_23.php.

1003. Rédaction, 'Quand la France se lance dans la reconnaissance faciale', 2 October 2019, Next INpact, https://www.nextinpact.com/article/29687/108256-quand-france-se-lance-dans-reconnaissance-faciale.

1004. Rédaction, 'Quand la France se lance dans la reconnaissance faciale', already mentioned.

1005. Cécile Crichton, 'Surveillance par drones : rappel à l'ordre de la CNIL', 20 January 2021, Dalloz Actualité, https://www.dalloz-actualite.fr/flash/surveillance-par-drones-rappel-l-ordre-de-cnil#results_box.

1006. Cécile Crichton, 'Surveillance par drones : rappel à l'ordre de la CNIL', already mentioned; CNIL, 'Drones : la CNIL sanctionne le ministère de l'Intérieur', 14 janvier 2021, https://www.cnil.fr/fr/drones-la-cnil-sanctionne-le-ministere-de-linterieur.

1007. Cécile Crichton, 'Surveillance par drones : rappel à l'ordre de la CNIL', already mentioned.

1008. Daphne Leprince-Ringuet, 'L'intérêt des services de police pour la reconnaissance faciale de plus en plus dénoncé', 11 September 2021, ZDNet, https://www.zdnet.fr/actualites/l-interet-des-services-de-police-pour-la-reconnaissance-faciale-de-plus-en-plus-denonce-39928887.htm.

1009. Translated from French: CNIL, 'La CNIL publie son avis sur le décret relatif à l'utilisation de la vidéo intelligente pour mesurer le port du masque dans les transports', 12 March 2021, https://www.cnil.fr/fr/avis-sur-le-decret-video-intelligente-port-du-masque.

1010. Rédaction, 'Quand la France se lance dans la reconnaissance faciale', 2 October 2019, Next INpact, https://www.nextinpact.com/article/29687/108256-quand-france-se-lance-dans-reconnaissance-faciale.

1011. On all these experiments see Rédaction, 'Quand la France se lance dans la reconnaissance faciale', already mentioned.

1012. Philippe Reltien, 'Reconnaissance faciale : officiellement interdite, elle se met peu à peu en place', 5 September 2020 (update), France Inter, https://www.franceinter.fr/reconnaissance-faciale-officiellement-interdite-elle-se-met-peu-a-peu-en-place. Francesco et al., Biometric and Behavioural Mass Surveillance in EU Member States, Report for the Greens/EFA in the European Parliament, 1 October 2021, p. 83 s., https://www.greens-efa.eu/biometricsurveillance/.

1013. Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 59.

1014. Philippe Reltien, 'Reconnaissance faciale : officiellement interdite, elle se met peu à peu en place', already mentioned.

1015. Decree n° 2019-452 of 13 May 2019 'autorisant la création d'un moyen d'identification électronique dénommé "Authentification en ligne certifiée sur mobile"', JORF n°0113 of 16 May 2019, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038475477/.

1016. Marc Rees, 'ALICEM : la biométrie de l'identité numérique sur mobile fait tiquer la CNIL', 16 May 2019, Next INpact, https://www.nextinpact.com/article/29403/107883-alicem-biometrie-identite-numerique-sur-mobile-fait-tiquer-cnil.

1017. Nathalie Silbert, 'Comment la reconnaissance faciale s'installe en France', 15 October 2019, Les Echos, https://www.lesechos.fr/tech-medias/intelligence-artificielle/comment-la-reconnaissance-faciale-sinstalle-en-france-1140171.

1018. Marc Rees, 'Cédric O imagine un lecteur de carte pour valider sa majorité à l'entrée des sites pornos', 19 July 2019, Next INpact, https://www.nextinpact.com/article/29543/108064-cedric-oimagine-lecteur-carte-pour-valider-sa-majorite-a-entree-sites-pornos.

1019. Deliberation n° 2018-342 of 18 October 2018 'portant avis sur projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé "Application de lecture de l'identité d'un citoyen en mobilité" (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile', demande d'avis n° 18008244, JORF n°0113 of 16 May 2019, text n° 81, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038475742.

1020. By default, the vast majority of mobile phones are «vendor locked». This means that the final user can only use the phone the way the vendor restricts this device in terms of use. The user has neither administrator rights, nor system access, and can only install applications from official marketplaces. «Rooting» a phone is necessary to give full access rights to the user. This requires installing a new operating system (such as lineageos), which will enable the user to gain full access to their device. Some devices are vendor-protected (especially through system signature and DRMs), and in such cases rooting a phone requires «jailbreaking» the phone, in order to gain the capability to install a customised Operating System.

1021. Marc Rees, 'Reconnaissance faciale : La Quadrature du Net attaque le décret ALICEM', 22 July 2019, Next INpact, https://www.nextinpact.com/article/29546/108065-reconnaissance-faciale-la-quadrature-net-attaque-decret-alicem. The application can be found at https://www.laquadrature.net/wp-content/uploads/sites/8/2019/07/1084951458_DECR_ALICEM_REQ.pdf.

1022. Asma Mhalla in Arrêt sur images, 15 November 2019, https://www.arretsurimages.net/emissions/arret-sur-images/reconnaissance-faciale-on-cree-laccoutumance?utm_source=gazette%2B-%2Babonn%C3%A9s&utm_campaign=b6e8015315-gazette_20191115&utm_medium=email&utm_term=0_bd520e065e-b6e8015315-195742417. During this interview, speakers are Olivier Tesquet, Asma Mhalla and Didier Baichere.

1023. On all this paragraph see Marc Rees, 'ALICEM : la biométrie de l'identité numérique sur mobile fait tiquer la CNIL', already mentioned.

1024. https://www.interieur.gouv.fr/Le-ministere/DGSI.

1025. https://www.dgse.gouv.fr/en.

1026. https://www.drsd.defense.gouv.fr/presentation-de-la-drsd-en.

1027. https://www.defense.gouv.fr/english/drm.

1028. https://www.douane.gouv.fr/fiche/la-direction-nationale-du-renseignement-et-des-enquetes-douanieres.

1029. https://www.economie.gouv.fr/tracfin.

1030. Estelle De Marco, 'France', in Sieber and Nicolas von zur Mühlen (eds.), Access to Telecommunication Data in Criminal Justice, A Comparative Analysis of European legal Orders, Max-Planck-Institut für Auslandisches und Internationales Strafrecht, Dincker & Humblot, Berlin, 2016, p. 435-498 [p. 444].

1031. Estelle De Marco, 'La captation des données', in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux, Institut Universitaire Varenne, coll. colloques et essais, 4th trim. 2017, p. 91-107 [p. 101-106].

1032. Estelle De Marco, 'La captation des données', already mentioned, p. 105.

1033. Estelle De Marco, 'La captation des données', already mentioned, p. 105.

1034. Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 48-49.

1035. Translated from French: Calach, 'Fichiers policiers version 2008 : STIC et JUDEX donnent naissance à ARIANE et snobent la CNIL', 10 January 2008, https://www.agoravox.fr/actualites/societe/article/fichiers-policiers-version-2008-34053; see also Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p. 50.

1036. Translated from French: Caroline Piquet, 'Stic, Judex, Taj: vous êtes peut-être déjà fichés par ces cousins du fichier TES', 2 November 2016, L'Express, https://www.lexpress.fr/actualite/societe/stic-judex-taj-vous-etes-peut-etre-deja-fiches-par-ces-cousins-du-fichier-tes_1846388.html; Marc Rees, Le méga-fichier TES visé par une procédure de référé suspension au Conseil d'État, 28 February 2017, Next INpact, https://www.nextinpact.com/article/25717/103475-le-mega-fichier-tes-vise-par-procedure-refere-suspension-au-conseil-d-etat.

1037. Translated from French: Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 48-49.

1038. Translated from French: Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, already mentioned, p.55. The author refers to a statement from François Pillet, reporter of the text before the Senate. By the end of the 19th Century, the same fear was expressed by the French public opinion in relation to the collection of photographs by public authorities. On this issue, see the introduction of the current report.

1039. Translated from French: see Olivier Tesquet, À la trace - Enquête sur les nouveaux territoires de la surveillance, ed. Premier Parallèle, 2020, p. 55. The author refers to the statement from 120 members of the French Parliament in their referral to the Constitutional Council. The act of referral is availble at https://www.conseil-constitutionnel.fr/les-decisions/decision-n-2012-652-dc-du-22-mars-2012-saisine-par-60-deputes.

1040. Deliberation n° 2016-292 of 29 September 2016 'portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (saisine n° 1979541)', JORF n°0254 of 30 October 2016, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033318979/.

1041. Conseil d'État, 10th-9th ch. réunies, 18 October 2018, 404996, Inédit au recueil Lebon, § 17, https://www.legifrance.gouv.fr/ceta/id/CETATEXT000037507135/.

1042. Marc Rees, 'Le méga-fichier TES visé par une procédure de référé suspension au Conseil d'État', 28 February 2017, Next INpact, https://www.nextinpact.com/article/25717/103475-le-mega-fichier-tes-vise-par-procedure-refere-suspension-au-conseil-d-etat.

1043. Jean-Marc Manach, 'Fichier des empreintes digitales : pourquoi la CNIL sanctionne le ministère de l'Intérieur', 30 September 2021, Next INpact, https://www.nextinpact.com/article/48268/fichier-empreintes-digitales-pourquoi-cnil-sanctionne-ministere-interieur; CNIL, 'Fichier automatisé des empreintes digitales : rappel à l'ordre du ministère de l'Intérieur', 30 September 2021, https://www.cnil.fr/fr/fichier-automatise-des-empreintes-digitales-rappel-lordre-du-ministere-de-linterieur.

1044. Businesscoot, 'Le marché des alarmes et de la vidéosurveillance: France', 24 November 2011 (update), https://www.businesscoot.com/fr/etude/le-marche-des-alarmes-et-de-la-videosurveillance-france.

1045. Translated from French: MSI, 'Marché de la Vidéosurveillance en France 2019', May 2021, https://www.msi-reports.com/market_research_report_pdfs/GFR12-S.pdf.

1046. . Agathe Albouy, 'Les systèmes de vidéosurveillance biométrique dans les supermarchés inquiètent', 5 June 2021, La Dépêche, https://www.ladepeche.fr/2021/06/04/les-systemes-de-videosurveillance-biometrique-dans-les-supermarches-inquietent-9585624.php; La Quadrature du Net, 'Vidéosurveillance biométrique dans nos supermarchés',

31 May 2021, https://www.laquadrature.net/2021/05/31/videosurveillance-biometrique-dans-nos-supermarches/.

1047. . La Quadrature du Net, 'Vidéosurveillance biométrique dans nos supermarchés', already mentioned.

1048. Delphine Cuny, 'La Soc Gen ose la reconnaissance biométrique faciale pour ouvrir un compte', 16 February 2018, La Tribune, https://www.latribune.fr/entreprises-finance/banques-finance/la-soc-gen-ose-la-reconnaissance-biometrique-faciale-pour-ouvrir-un-compte-768743.html.

1049. Delphine Cuny, 'La Soc Gen ose la reconnaissance biométrique faciale pour ouvrir un compte', already mentioned.

1050. CNIL, 'Les dispositifs biométriques pour l'accès aux cantines scolaires', 18 August 2021, https://www.cnil.fr/fr/les-dispositifs-biometriques-pour-lacces-aux-cantines-scolaires.

1051. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 35 s., https://hal.archives-ouvertes.fr/tel-02439529.

1052. Translated from French: Guillaume Gormand, already mentioned, p. 41.

1053. Translated from French: Guillaume Gormand, already mentioned, p. 41.

1054. Guillaume Gormand, already mentioned, p. 37-38.

1055. Translated from French: Guillaume Gormand, already mentioned, p. 45.

1056. Translated from French: Guillaume Gormand, already mentioned, p. 48.

1057. François Sureau, Sans la liberté, Tracts Gallimard n°8, 2019, p. 6 and p. 31; Jacques Robert and Jean Duffar, Droits de l'homme et libertés fondamentales, Montchrestien, Lextenso éditions, 8th ed., 2009, p. 2; Olivier Tesquet, Etat d'urgence technologique, Premier Parallèle, 2021, p. 11-12; David Lyon, Surveillance Studies: An Overview, ed. Polity, 2007, p. 5.

1058. Translated from French: Marylou Magal, 'Covid-19 : un rapport du Sénat préconise la collecte de données personnelles pour prévenir les crises sanitaires', 3 June 2021, Public Sénat, https://www.publicsenat.fr/article/societe/covid-19-un-rapport-du-senat-preconise-la-collecte-de-donnees-personnelles-pour.

1059. Marc Rees, 'Interdiction de la reconnaissance faciale : Muselier, Estrosi et Ciotti furieux contre la CNIL', 29 October 2019, Next INpact, https://www.nextinpact.com/article/29759/108348-interdiction-reconnaissance-faciale-muselier-estrosi-et-ciotti-furieux-contre-cnil.

1060. Translated from French: Marc Rees, 'Interdiction de la reconnaissance faciale : Muselier, Estrosi et Ciotti furieux contre la CNIL', 29 October 2019, Next INpact, https://www.nextinpact.com/article/29759/108348-interdiction-reconnaissance-faciale-muselier-estrosi-et-ciotti-furieux-contre-cnil.

1061. La Quadrature du Net, 'La reconnaissance faciale des manifestant.es est déjà autorisée', 18 November 2019, https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/.

1062. Translated from French: Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, already mentioned, p. 51.

1063. François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, Tallandier Essais, 2019, p. 43.

1064. François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, already mentioned, p.43, footnote 24.

1065. François Sureau, 'Le refus de sacrifier la liberté', Interview from Fabien Escalona and Ellen Salvi for Mediapart, 10 October 19, https://www.april.org/le-refus-de-sacrifier-la-liberte-francois-sureau (transcript) and https://www.youtube.com/watch?v=yYY-B0jZMD4&t=7s (video).

1066. See subsection 7.1.1 1. of the current study.

1067. Estelle De Marco, 'La captation des données', in Katarzyna Blay-Grabarczyk and Laure Milano (dir.), Le nouveau cadre législatif de la lutte contre le terrorisme à l'épreuve des droits fondamentaux, Institut Universitaire Varenne, coll. colloques et essais, 4th trim. 2017, p. 91-107 [p. 104].

1068. Emile Marzolf, 'Avec son livre blanc sur la sécurité, l'Intérieur compte franchir le "mur technologique"', 24 novembre 2020, Acteurs Publics, https://www.acteurspublics.fr/articles/avec-son-livre-blanc-sur-la-securite-linterieur-compte-franchir-le-mur-technologique.

1069. . Martin Untersinger, 'Cédric O : "Expérimenter la reconnaissance faciale est nécessaire pour que nos industriels progressent", 14 October 2019, Le Monde, https://www.lemonde.fr/economie/article/2019/10/14/cedric-o-experimenter-la-reconnaissance-faciale-est-necessaire-pour-que-nos-industriels-progressent_6015395_3234.html.

1070. L'OBS with AFP, 'Reconnaissance faciale: le pas de deux compliqué des groupes technologiques et des forces de l'ordre', 17 June 2020, https://www.nouvelobs.com/societe/20200617.AFP7785/reconnaissance-faciale-le-pas-de-deux-complique-des-groupes-technologiques-et-des-forces-de-l-ordre.html; Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', Note du CREOGN, September 2019, p. 4, https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-creogn/reconnaissance-faciale-et-controles-preventifs-sur-la-voie-publique-l-enjeu-de-l-acceptabilite.

1071. Pierre Januel, 'Police : l'utilisation massive de la reconnaissance faciale se confirme', 19 October 2020, Next INpact, https://www.nextinpact.com/article/44242/police-utilisation-massive-reconnaissance-faciale-se-confirme#/page/2.

1072. Translated from French: Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, already mentioned, p. 39.

1073. Translated from French: Rédaction, 'Quand la France se lance dans la reconnaissance faciale', 2 Octobre 2019, Next INpact, https://www.nextinpact.com/article/29687/108256-quand-france-se-lance-dans-reconnaissance-faciale.

1074. Translated from French: Philippe Reltien et Cellule investigation de Radio France, Quand la reconnaissance faciale en France avance masquée, 4 September 2020, https://www.franceculture.fr/societe/quand-la-reconnaissance-faciale-en-france-avance-masquee.

1075. The French Constitution is available in English at https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/anglais/constiution_anglais_oct2009.pdf. The 1789 Declaration on Human and Citizens' rights is available in English at https://constitutionnet.org/sites/default/files/declaration_of_the_rights_of_man_1789.pdf.

1076. Chart of signatures and ratifications of Treaty 005, Convention for the Protection of Human Rights and Fundamental Freedoms, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005?module=signatures-by-treaty&treatynum=005.

1077. Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', in Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet (dir.), Libertés et droits fondamentaux, Dalloz, 11th ed., 2005, p. 39, n° 68. The second part of the text does not receive application because the principle of reciprocity does not apply as regards the ECHR.

1078. Frédéric Sudre, already mentioned, p.39, n° 69.

1079. Law n° 78-17 of 6 January 1978 'relative à l'informatique, aux fichiers et aux libertés', https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624/2019-06-04/.

1080. CNIL, 'Les missions de la CNIL', https://www.cnil.fr/fr/les-missions-de-la-cnil. .

1081. https://www.cnctr.fr/

1082. See, on the CNIL website, the information pages https://www.cnil.fr/fr/videosurveillance-videoprotection, https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique, and https://www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables.

1083. Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, already mentioned, p. 45; Colonel Dominique Schoenher, 'Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité', Note du CREOGN, September 2019, p. 4, https://www.gendarmerie.interieur.gouv.fr/crgn/publications/les-notes-du-creogn/reconnaissance-faciale-et-controles-preventifs-sur-la-voie-publique-l-enjeu-de-l-acceptabilite; Eric Töpfer, 'Urban Video Surveillance in Europe: A Political Choice?', in European Forum for Urban Security, Citizens, Cities and Video Surveillance - Towards a democratic and responsible use of CCTV, June 2010, p. 65-79, p. 78, https://panoptykon.org/sites/panoptykon.org/files/cctv_publication_en_0.pdf.

1084. Articles L.223-1 to L.223-9 of the ISC, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025505235/#LEGISCTA000025508305, and Articles L.251-1 to L.255-1 of the CSI, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025505402/#LEGISCTA000025508192.

1085. Articles L.251-1 s. of the ISC, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025505402/#LEGISCTA000025508192.

1086. Guillaume Gormand shows that, in certain monitored area of Montpellier, only 14% of individuals are aware of the existence of cameras: Guillaume Gormand, L'évaluation des politiques publiques de sécurité : résultats et enseignements de l'étude d'un programme de vidéosurveillance de la Ville de Montpellier, Droit, Université Grenoble Alpes, 2017, NNT: 2017GREAD014, p. 345, https://hal.archives-ouvertes.fr/tel-02439529.

1087. Article L.241-1 of the ISC, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025505308/#LEGISCTA000032656298.

1088. Article L.251-5 of the ISC, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000025505416/.

1089. Article L.223-4 of the ISC, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000025505244/.

1090. CNIL, 'Le droit d'accès aux fichiers de police, de gendarmerie et de renseignement', 18 June 2019, https://www.cnil.fr/fr/le-droit-dacces-aux-fichiers-de-police-de-gendarmerie-et-de-renseignement. .

1091. Guilhem Marois, 'Le contrôle des services de renseignement en France', Thesis, Law, University of Bordeaux, 18 December 2019, NNT : 2019BORD0417, n° 429, https://tel.archives-ouvertes.fr/tel-02497072.

1092. Guilhem Marois, 'Le contrôle des services de renseignement en France', already mentioned, n° 159 s.

1093. Guilhem Marois, 'Le contrôle des services de renseignement en France', already mentioned, n° 176-189.

1094. Translated from French: CNIL, 'Reconnaissance faciale : pour un débat à la hauteur des enjeux', 15 November 2019, https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf.

1095. https://www.privacyinternational.org/location/united-kingdom.

1096. https://www.liberties.eu/en/about/organisation.

1097. See the previous subsections relating to France.

1098. https://technopolice.fr/.

1099. Translated from French: La Quadrature du Net, 'La Quadrature du Net ouvre la bataille contre la technopolice', 16 September 2019, https://www.laquadrature.net/2019/09/16/la-quadrature-du-net-ouvre-la-bataille-contre-la-technopolice/.

1100. Translated from French: La Quadrature du Net, 'La Quadrature du Net ouvre la bataille contre la technopolice', already mentioned.

1101. Ministère de l'Intérieur, 'La nouvelle carte nationale d'identité', 3 May 2021, https://www.interieur.gouv.fr/actualites/actu-du-ministere/nouvelle-carte-nationale-didentite: on this webpage, the French Ministry of Home Affairs states: "the new identity card will be more secure [and] more practical".

1102. Friedrich A. Hayek, 'The Road to Serfdom', in The Road to Serfdom with The Intellectuals and Socialism, Institute of Economic Affairs, 2005, p. 69, https://cdn.mises.org/Road%20to%20serfdom.pdf.

1103. Translated from French: François Sureau, Pour la liberté – Répondre au terrorisme sans perdre la raison, Tallandier Essais, 2019, p.43. On the prevention of totalitarianism through culture and self-identity, see also Michael J. Griffin and Tom Moylan, Exploring the Utopian impulse: Essays on utopian thought and practice, Peter Lang AG, International Academic Publishers, Bern 2007, p. 52.

1104. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 76-95.

1105. Identity Documents Act 2010, https://www.legislation.gov.uk/ukpga/2010/40/contents/enacted.

1106. HM Passport Office, 'Privacy information notice' (accessible version), https://www.gov.uk/government/statistics/hmpo-privacy-information-notice/privacy-information-notice-accessible-version.

1107. Gov.uk, 'About us', https://www.gov.uk/government/organisations/hm-passport-office/about.

1108. .Home Office, 'Biometric information: introduction', Version 6.0, 10 November 2019, p. 6, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/847376/biometric-information-introduction-6.0.pdf.

1109. .Home Office, 'Biometric information: introduction', Version 6.0, already mentioned.

1110. .Home Office, 'Biometric information: introduction', Version 6.0, already mentioned.

1111. .Parliamentary questions, Answer given by Ms Johansson on behalf of the European Commission to question E-000334/2021 of Cornelia Ernst (The Left) on the British stored material in SIS II and at Europol, 6 April 2021, https://www.europarl.europa.eu/doceo/document/E-9-2021-000334-ASW_EN.html.

1112. . Jennifer Rankin, 'UK accused of 'behaving like cowboys' over EU database copying', 9 January 2020, The Guardian, https://www.theguardian.com/world/2020/jan/09/uk-accused-of-behaving-like-cowboys-over-eu-database-copying. The author refers to a document first reported by Nikolaj Nielsen, UK unlawfully copying data from EU police system, 28 May 2018, EUObserver https://euobserver.com/justice/141919.

1113. Paul Bischoff, 'Surveillance camera statistics: which cities have the most CCTV cameras?', 17 May 2021, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ . See also Ma Forteresse, 'Vidéosurveillance : Histoire de la caméra de surveillance', https://www.maforteresse.com/guide/videosurveillance-histoire-de-la-camera-de-surveillance.html#Quelques_chiffres_sur_lutilisation_actuelle_de_la_camera_de_surveillance, which evokes a ratio of 68,4 cameras for 1,000 inhabitants.

1114. Paul Bischoff, 'Surveillance camera statistics: which cities have the most CCTV cameras?', already mentioned.

1115. .Court of Appeal (civil division), Queen's Bench Division (Administrative Court), Cardiff District Registry, [2020] EWCA Civ 1058, 11 August 2020, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

1116. .High Court of Justice, Queen's Bench Division, Divisional Court, Cardiff Civil Justice Centre, [2019] EWHC 2341 (Admin), 4 September 2019, https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf.

1117. . Samuel White, 'London Metropolitan Police Will Deploy Live Facial Recognition Systems', 27 January 2020, The Internet Protocol, https://internetprotocol.co/hype-news/2020/01/27/the-met-to-deploy-facial-recognition-cameras/. See also Vikram Dodd, 'Met police to begin using live facial recognition cameras in London', 24 January 2020, https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras?CMP=fb_a-technology_b-gdntech.

1118. Metropolitan Police, 'Live Facial Recognition', https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/?__cf_chl_captcha_tk__=vUCzIM5P3XxhJNasZ22YLAfYok5XR86qx0c8qZNKhEk-1637655891-0-gaNycGzNBz0.

1119. Metropolitan Police, 'About the camera', https://www.met.police.uk/advice/advice-and-information/bwv/body-worn-video-bwv/about-the-camera/. The Axon website is available at https://uk.axon.com.

1120. Metropolitan Police, 'Body Worn Video (BWV)', https://www.met.police.uk/advice/advice-and-information/bwv/body-worn-video-bwv/.

1121. DTS Solutions, 'Lancashire Constabulary deploys Motorola solutions VB400 body-worn cameras', https://dts.solutions/lancashire-constabulary-vb400-case-study/.

1122. . Kurt Zindulka, 'Definitely Not Authoritarian: Britain to Introduce Facial Recognition App for Government Services', 14 October 2021, Breitbart, https://www.breitbart.com/europe/2021/10/14/definitely-not-authoritarian-uk-to-use-facial-recognition-for-govt-services/. The Author reports a testimony from the director of the civil liberties campaign group Big Brother Watch, Silke Carlo, before the Committee on Justice and Home Affairs in the House of Lords.

1123. Paul Bischoff, 'Biometric data: 96 countries ranked by how they're collecting it and what they're doing with it', 27 January 2021, Comparitech, https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/.

1124. Rob Davies, 'NHS app storing facial verification data via contract with firm linked to Tory donors', 15 September 2021, The Guardian, https://www.theguardian.com/society/2021/sep/15/nhs-app-storing-facial-verification-data-via-contract-with-firm-linked-to-tory-donors. .

1125. Neil Campbell, 'UK Vaccine Passport App Sends Biometric Facial Recognition Data to Private Company, Shares With Law Enforcement', 20 September 2021, Vision Times, https://www.visiontimes.com/2021/09/20/uk-vaccine-passport-app-biometric-facial-recognition.html.

1126. Rob Davies, 'NHS app storing facial verification data via contract with firm linked to Tory donors', already mentioned.

1127. Neil Campbell, 'UK Vaccine Passport App Sends Biometric Facial Recognition Data to Private Company, Shares With Law Enforcement', already mentioned.

1128. Rob Davies, 'NHS app storing facial verification data via contract with firm linked to Tory donors', already mentioned.

1129. Rob Davies, 'NHS app storing facial verification data via contract with firm linked to Tory donors', already mentioned.

1130. . Kurt Zindulka, 'Definitely Not Authoritarian: Britain to Introduce Facial Recognition App for Government Services', 14 October 2021, Breitbart, https://www.breitbart.com/europe/2021/10/14/definitely-not-authoritarian-uk-to-use-facial-recognition-for-govt-services/.

1131. . Mike Wright and Harry Yorke, 'New Gov.uk app will let people access 300 services at the blink of an eye', 13 October 2021, The Telegraph, https://www.telegraph.co.uk/politics/2021/10/13/new-govuk-app-will-let-people-access-300-services-blink-eye/.

1132. . Mike Wright and Harry Yorke, 'New Gov.uk app will let people access 300 services at the blink of an eye', already mentioned.

1133. Gov.uk, 'National Insurance', https://www.gov.uk/national-insurance/your-national-insurance-number.

1134. Security Service MI5, 'What is the difference between MI5 and MI6 (SIS)?' in FAQ about MI5, https://www.mi5.gov.uk/faq/what-is-the-difference-between-mi5-and-mi6-sis.

1135. Security Service MI5, 'What is the difference between MI5 and MI6 (SIS)?', already mentioned.

1136. Gov.uk, 'Government Communications Headquarters', https://www.gov.uk/government/organisations/government-communications-headquarters. See also GCHQ, 'Our mission to help keep the UK safe', 12 June 2021 (update), https://www.gchq.gov.uk/information/welcome-to-gchq.

1137. Investigatory Powers Tribunal, 5 December 2014, [2014] UKIPTrib 13_77-H, §15, https://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf. See also ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, appl. n° 58170/13, 62322/14, 24960/15, § 103, http://hudoc.echr.coe.int/eng?i=001-210077

1138. Investigatory Powers Tribunal, 5 December 2014, [2014] UKIPTrib 13_77-H, already mentioned, §15. National Security Agency, UK-USA Agreement Release, 1940-1956, https://web.archive.org/web/20130805231226/http://www.nsa.gov/public_info/declass/ukusa.shtml.

1139. Immanuel Jotham, 'British intelligence agencies may have been collecting and sharing your social media data', 18 October 2017, International Business Time, https://www.ibtimes.co.uk/british-intelligence-agencies-may-have-been-collecting-sharing-your-social-media-data-1643597. See also Owen Bowcott, 'UK spy agencies may be circumventing data-sharing law, tribunal told', 17 October 2017, The Guardian, https://www.theguardian.com/technology/2017/oct/17/uk-spy-agencies-intelligence-mi5-mi6-law-data-sharing-tribunal.

1140. "PRISM was a programme through which the United States' Government obtained intelligence material (such as communications) from Internet Service Providers ("ISPs"). Access under PRISM was specific and targeted (as opposed to a broad "data mining" capability). The United States' administration stated that the programme was regulated under the Foreign Intelligence Surveillance Act ("FISA"), and applications for access to material through PRISM had to be approved by the Foreign Intelligence Surveillance Court ("FISC")". ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, appl. n° 58170/13, 62322/14, 24960/15, § 23, http://hudoc.echr.coe.int/eng?i=001-210077.

1141. "According to the leaked documents, the Upstream programme allowed the collection of content and communications data from fibre optic cables and infrastructure owned by United States'" communications service providers (CSPs). "This programme had broad access to global data, in particular that of non-US citizens, which could then be collected, stored and searched using keywords": ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, already mentioned, § 25.

1142. Investigatory Powers Tribunal, 5 December 2014, [2014] UKIPTrib 13_77-H, already mentioned, §4.

1143. Investigatory Powers Tribunal, 5 December 2014, [2014] UKIPTrib 13_77-H, already mentioned, §23.

1144. ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, appl. n° 58170/13, 62322/14, 24960/15, § 16, http://hudoc.echr.coe.int/eng?i=001-210077.

1145. Investigatory Powers Tribunal, 29 July 2016, [2016] UKIPTrib 15_110-CH, §73, https://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf.

1146. Investigatory Powers Tribunal, 29 July 2016, [2016] UKIPTrib 15_110-CH, already mentioned, §84 and §102.

1147. Investigatory Powers Tribunal, 29 July 2016, [2016] UKIPTrib 15_110-CH, already mentioned, §4. See also Owen Bowcott and Richard Norton-Taylor, 'UK spy agencies have collected bulk personal data since 1990s, files show', 21 April 2016, The Guardian, https://www.theguardian.com/world/2016/apr/21/uk-spy-agencies-collected-bulk-personal-data-since-1990s.

1148. ECtHR, gr. ch., 25 May 2021, Big Brother Watch and others v. The United Kingdom, already mentioned, § 425.

1149. See for example Security Service MI5, Bulk Data, https://www.mi5.gov.uk/bulk-data.

1150. Gov.uk, 'Investigatory Powers Act 2016 – codes of practice', https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

1151. Graham Smith, 'The UK Investigatory Powers Act 2016 – what it will mean for your business', November 2016, Bird & Bird, https://www.twobirds.com/en/news/articles/2016/uk/what-the-investigatory-powers-bill-would-mean-for-your-business; Ewen MacAskill, 'Extreme surveillance' becomes UK law with barely a whimper', 19 November 2016, The Guardian, https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.

1152. 'Liberty, Legal challenge: Investigatory Powers Act', https://www.libertyhumanrights.org.uk/issue/legal-challenge-investigatory-powers-act/.

1153. Investigatory Powers Tribunal, 12 February 2016, [2016] UKIP Trib 14_85-CH, §3, https://www.ipt-uk.com/docs/Privacy_Greennet_and_Sec_of_State.pdf.

1154. Investigatory Powers Tribunal, 12 February 2016, [2016] UKIP Trib 14_85-CH, already mentioned, §9.

1155. Investigatory Powers Tribunal, 12 February 2016, [2016] UKIP Trib 14_85-CH, already mentioned, §5.

1156. Gov.uk, 'Investigatory Powers Act 2016 – codes of practice', https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice; see also Gov.uk, RIPA codes, https://www.gov.uk/government/collections/ripa-codes.

1157. Paul Lewis, David Conn and David Pegg, 'UK government using confidential patient data in coronavirus response', 12 April 2020, The Guardian, https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response.

1158. . Mary Fitzgerald and Cori Crider, 'We need answers about the five-year NHS data deals with big tech', 4 December 2020, Open Democracy, https://www.opendemocracy.net/en/ournhs/we-need-answers-about-five-year-nhs-data-deals-big-tech/; Mary Fitzgerald and Cori Crider, 'We've won our lawsuit over Matt Hancock's £23m NHS data deal with Palantir', 30 March 2021, Open Democracy, https://www.opendemocracy.net/en/ournhs/weve-won-our-lawsuit-over-matt-hancocks-23m-nhs-data-deal-with-palantir/.

1159. . ICO, 'Enforcement notice to Her Majesty's Revenue and Customs', 9 May 2019, §1, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2614924/hmrc-en-201905.pdf.

1160. . ICO, 'Enforcement notice to Her Majesty's Revenue and Customs', already mentioned, §12-23.

1161. . ICO, 'Enforcement notice to Her Majesty's Revenue and Customs', already mentioned, Annex 1. See also Nana Ama SarfoForbes, 'Efficiency Vs. Privacy: The Debate Over Biometric Tax Data', 23 February 2021, https://www.forbes.com/sites/taxnotes/2021/02/23/efficiency-vs-privacy-the-debate-over-biometric-tax-data/.

1162. . Peter Fry, 'How many cameras are there?', 18 June 2008, https://web.archive.org/web/20081023191646/http://www.cctvusergroup.com/art.php?art=94.

1163. . By Ivana Davidovic, 'Should we be worried by ever more CCTV cameras?', 18 November 2019, BBC, https://www.bbc.com/news/business-50348861.

1164. For example, the provider of the "Causeway Donseed biometric labour management solution" states that this solution "is trusted by the full range of construction contractors – from main contractors to growing specialist sub-contractors – and is currently used on more than 2,000 construction sites across the UK and Ireland": Donseed, 'Industry Leading Fingerprint Recognition and Non-Contact Facial Recognition Technology for Construction Contractors', https://www.donseed.com/?utm_source=UK%20Construction%20Media&utm_medium=Editorial&utm_campaign=UK%20CM%20Newsletter%20Feature. See also UK Construction online, 'A look at how construction companies are using biometric technology to replace paper timesheets', 29 March 2018, https://www.ukconstructionmedia.co.uk/features/look-construction-companies-using-biometric-technology-replace-paper-timesheets/. See also Katya Pivcevic, 'Construction site biometrics advance with Biosite contract and new Redrock product', 8 January 2021, Biometric Update.com, https://www.biometricupdate.com/202101/construction-site-biometrics-advance-with-biosite-contract-and-new-redrock-product.

1165. Justin Lee, 'CSC report finds that 25% of U.K. retailers use facial recognition in store', 14 September 2015, Biometric Update.com, https://www.biometricupdate.com/201509/csc-report-finds-that-25-of-u-k-retailers-use-facial-recognition-in-store.

1166. Abigail Beall, 'UK's first biometric supermarket lets you pay using the veins in your hand', 20 September 2017, Alphr, https://www.alphr.com/technology/1007091/fingopay-supermarket-uk-vein-payment/. The author refers to the "Costcutters at Brunel University in London", which uses "technology developed by a company called Sthaler". The author explains that "a finger scanner is fitted at the till and is used to retrieve the person's bank card details, using payment provider Worldpay".

1167. NatWest Group, 'Behavioural biometrics set to replace bank passwords', 15 June 2020, https://www.rbs.com/rbs/news/2020/06/behavioural-biometrics-set-to-replace-bank-passwords.html.

1168. Department for education, Protection of biometric information of children in schools and colleges, March 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/692116/Protection_of_Biometric_Information.pdf.

1169. Frauke Brodkorb-Kettenbach, 'Pay with your face – at the school cafeteria!', 22 October 2021, https://www.food-service.de/international/int-news/face-recognition--uk-pay-with-your-face--at-the-school-cafeteria-49650.

1170. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 79-80.

1171. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 80.

1172. . Laurent Laniel et Pierre Piazza, 'Une carte nationale d'identité biométrique pour les Britanniques : l'antiterrorisme au cœur des discours de justification', in Cultures & Conflits, n°64, Hiver 2006, p.49-63, n° 5, https://doi.org/10.4000/conflits.2174.

1173. . Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p. 81. See also Laurent Laniel et Pierre Piazza, 'Une carte nationale d'identité biométrique pour les Britanniques : l'antiterrorisme au cœur des discours de justification', already mentioned, n° 5.

1174. . Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p. 81.

1175. . Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p. 80.

1176. . Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p. 82.

1177. . Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, already mentioned, p. xviii.

1178. . John Lettice, 'UK EU presidency aims for Europe-wide biometric ID card', 13 July 2005, The Register, https://www.theregister.com/2005/07/13/uk_eu_id_proposal/.

1179. Investigatory Powers Tribunal, 29 July 2016, [2016] UKIPTrib 15_110-CH, §70, https://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf. See especially §70: "it seems difficult to conclude that the use of BCD was foreseeable by the public, when it was not explained to Parliament;

and several opportunities arose when legislation or Codes of Practice were being introduced or amended (and particularly in 2000 when s.80 of RIPA was passed), when the government of the day did not avow the use of s.94".

1180. Alan Travis, 'Police told to delete on request millions of images of innocent people', 24 February 2017, The Guardian, https://www.theguardian.com/uk-news/2017/feb/24/police-told-to-delete-on-request-images-of-innocent-people; James Meikle, 'Police may have to destroy photos of innocent people after court ruling', 22 June 2012, The Guardian, https://www.theguardian.com/uk/2012/jun/22/police-photos-innocent-court-ruling.

1181. Alan Travis, 'Police told to delete on request millions of images of innocent people', already mentioned.

1182. Alan Travis, 'Police told to delete on request millions of images of innocent people', already mentioned; Rob Evans, Files detailing police spying operations against protesters published online, 14 January 2016, The Guardian, https://www.theguardian.com/uk-news/undercover-with-paul-lewis-and-rob-evans/2016/jan/14/files-detailing-police-spying-operations-against-protesters-published-online.

1183. Paul Wiles, Commissioner for the retention and use of biometric material, annual report 2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/644755/CCS207_CCS0917991760-1_Biometrics_Commissioner_ARA_Accessible.pdf. Citations can be respectively found n° 300, 304 and 303.

1184. Margi Murphy, 'Facial recognition to be ramped up across British borders', 29 June 2018, The Telegraph, https://www.telegraph.co.uk/technology/2018/06/29/facial-recognition-ramped-across-british-borders/.

1185. Home Office, Biometrics Strategy: Better public services, Maintaining public trust, June 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf.

1186. See subsection 7.2.1.1 of the current report.

1187. .Gov.uk, Closed consultation, 'Surveillance camera code of practice', Consultation runs from 9am on 13 August 2021 to 11:45pm on 8 September 2021, https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice;

1188. .Emma Woollacott, 'UK Government Accused Of Sneaking Through New Live Facial Recognition Rules', 23 August 2021, Forbes, https://www.forbes.com/sites/emmawoollacott/2021/08/23/uk-government-accused-of-sneaking-through-new-live-facial-recognition-rules/.

1189. .Emma Woollacott, 'UK Government Accused Of Sneaking Through New Live Facial Recognition Rules', already mentioned.

1190. Ellen Castelow, The Constitution of the United Kingdom, https://www.historic-uk.com/HistoryUK/HistoryofBritain/British-Constitution/. .

1191. Human Rights Act 1998, Introductory Text, https://www.legislation.gov.uk/ukpga/1998/42/contents.

1192. Human Rights Act 1998, Introduction, 1. The Convention Rights.

1193. Human Rights Act 1998, Introduction, 2. Interpretation of Convention rights.

1194. Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

1195. Information Commissioner's Opinion, The use of live facial recognition technology by law enforcement in public places, 31 October 2019, https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

1196. Information Commissioner's Opinion, The use of live facial recognition technology by law enforcement in public places, 31 October 2019, p. 2, https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

1197. See subsection 7.2.1.2.1 of the current study.

1198. Privacy International, 'National Security Certificates: Broad exemptions from the data protection regime will have consequences for our data protection rights and for adequacy', 3 November 2017, https://privacyinternational.org/news-analysis/1862/national-security-certificates-broad-exemptions-data-protection-regime-will-have.

1199. https://www.legislation.gov.uk/ukpga/1989/5/contents.

1200. https://www.legislation.gov.uk/en/ukpga/1994/13.

1201. https://www.legislation.gov.uk/ukpga/2000/23/contents.

1202. https://www.gov.uk/government/collections/ripa-codes. See also Security Service MI5, 'How MI5 gather intelligence', https://www.mi5.gov.uk/gathering-intelligence.

1203. Security Service MI5, MI5's Law and Governance, https://www.mi5.gov.uk/law-and-governance.

1204. https://www.mi5.gov.uk/interception-of-communications.

1205. https://www.mi5.gov.uk/covert-surveillance.

1206. https://www.mi5.gov.uk/covert-human-intelligence-sources.

1207. https://www.mi5.gov.uk/equipment-interference.

1208. https://www.mi5.gov.uk/bulk-data.

1209. Home Office, Surveillance Code of Practice, June 2013, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

1210. See subsection 7.2.1.3 of the current study.

1211. https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

1212. See subsection 7.2.1.2.1 of the current study.

1213. https://www.legislation.gov.uk/ukpga/2000/11/contents.

1214. https://www.legislation.gov.uk/ukpga/2001/24/contents.

1215. https://www.legislation.gov.uk/ukpga/2006/11/contents.

1216. https://www.legislation.gov.uk/ukpga/2008/28/contents.

1217. https://www.legislation.gov.uk/ukpga/2011/23/contents/enacted.

1218. Metropolitan Police, 'Live facial recognition', https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/?__cf_chl_captcha_tk__=36ul4U7Mo5.5SjL8ABMjFk.Bvqzp.zNN1y6h0J6U_Zo-1637933619-0-gaNycGzNB70.

1219. https://www.ipco.org.uk/.

1220. Tony Porter, 'Survey of Local Authorities Compliance with the Protection of Freedoms Act 2012', 20 October 2020, https://videosurveillance.blog.gov.uk/2020/10/20/survey-of-local-authorities-compliance-with-the-protection-of-freedoms-act-2012/.

1221. https://www.privacyinternational.org/location/united-kingdom.

1222. https://www.liberties.eu/en/about/organisation.

1223. https://www.statewatch.org/observatories/uk-civil-liberties-legislation/.

1224. See the previous subsections relating to the United Kingdom.

1225. House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, 25 February 2015, HC° 734, n° 63, https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/734/734.pdf.

1226. House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, already mentioned, n° 63. The report refers to a testimony of Professor van Zoonen. She bases her statement on the outcomes of her IMPRINTS research group, which conducted a survey in 2014.

1227. See also Jim Nash, 'Public facial recognition so far penned in by trust issues in the UK and Ireland', 22 September 2021, https://www.biometricupdate.com/202109/public-facial-recognition-so-far-penned-in-by-trust-issues-in-the-uk-and-ireland.

1228. House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, already mentioned, n° 62.

1229. House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, already mentioned, n° 68.

1230. House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, already mentioned, n° 70.

1231. House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, already mentioned, n° 71. The Committee refers to a testimony of Professor Martyn Thomas, which can be found in House of Commons Science and Technology Committee, Identity Card Technologies: Scientific Advice, Risk and Evidence, Sixth Report of Session 2005–06, HC 1032, n°131 p. 53, https://publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032.pdf.

1232. Edgar A. Whitley and Gus Hosein, Global Challenges for Identity Policies, ed. Palgrave Macmillan, 2010, p. 79.

1233. European Agency for fundamental Rights, Under watchful eyes: biometrics, EU IT systems and fundamental rights, 2018, p. 26, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf.

1234. Roberta Kostadinova, 'Romania: Shaping digital future with new electronic ID cards', 4 August 2020, https://www.trendingtopics.eu/romania-shaping-digital-future-with-new-electronic-id-cards/.

1235. Simona Fodor, 'Pilot project: Romania starts issuing eID cards', 3 August 2021, https://www.romania-insider.com/pilot-project-electronic-id-cards-aug-2021.

1236. Regulation (EU) 2019/1157 of 20 June 2019 on strengthening the security of identity cards, article 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R1157.

1237. Ro insider, 'RO president promulgates legislation introducing electronic ID cards', 4 August 2020, https://www.romania-insider.com/electronic-id-cards-legislation-aug-2020.

1238. Regulation (EU) 2019/1157 of 20 June 2019, already mentioned., art. 10.

1239. Translated from Romanian. Juridice.co, 'Critici la adresa proiectului SII Analytics. Reacția SRI. UPDATE: Finalizarea proiectului', 13 June 2019, https://www.juridice.ro/460184/critici-la-adresa-proiectului-sii-analytics.html.

1240. European Agency for fundamental Rights, Under watchful eyes: biometrics, EU IT systems and fundamental rights, 2018, p. 23, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf.

1241. European Agency for Fundamental Rights, already mentioned, p. 40.

1242. Alina Grigoras, Romania to have access to the European fingerprints database, 23 April 2015, https://www.romaniajournal.ro/society-people/romania-to-have-access-to-the-european-fingerprints-database/.

1243. Alina Grigoras, Romania to have access to the European fingerprints database, already mentioned.

1244. Romania is never named in the studies we accessed during the preparation of the current report.

1245. Ro Insider, 'Bucharest district sets up surveillance cameras to discourage illegal waste dumping', 11 July 2019, https://www.romania-insider.com/district-1-cameras-waste-dumping.

1246. Elko, 'Video surveillance system for Slatina city in Romania', https://www.elkogroup.com/cases/video-surveillance-system-for-slatina-city-in-romania.

1247. https://www.elkogroup.com/about.

1248. Paul Bischoff, 'Biometric data: 96 countries ranked by how they're collecting it and what they're doing with it', 27 January 2021, https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/.

1249. See, on the Motorola Solutions website, 'Romanian Police to Invest in 12,000 Body-worn Cameras from

Motorola Solutions', 16 July 2020, https://newsroom.motorolasolutions.com/news/romanian-police-to-invest-in-12000-body-worn-cameras-from-motorola-solutions.htm, and 'VB400 Body-Worn Camera', https://www.motorolasolutions.com/en_xu/video-security-access-control/body-worn-cameras/vb400.html.

1250. 'Romanian Border Police Invest in Safety at Their Borders', 14 December 2020, https://www.businesswire.com/news/home/20201214005078/en/Romanian-Border-Police-Invest-in-Safety-at-Their-Borders.

1251. Irina Marica, 'Romanian police could use body cameras to record talks with drivers', 13 June 2017, Romania Insider, https://www.romania-insider.com/police-officers-record-body-cameras-2017/.

1252. Adrian Vasilache, 'Mai multe ONG-uri cer ca Poliția să renunțe la actuala achiziție a unui sistem IT de recunoaștere facială', 8 October 2019, Hotnews https://economie.hotnews.ro/stiri-telecom-23412826-mai-multe-ong-uri-cer-politia-renunte-actuala-achizitie-unui-sistem-recunoastere-faciala.htm and a short article in English: Romania Insider, 'Romanian Police wants to implement national face recognition system, 30 September 2016, Romania Insider, https://www.romania-insider.com/romanian-police-wants-implement-national-face-recognition-system/.

1253. Adrian Vasilache, 'Poliția Română încearcă, din nou, să-și dezvolte propriul sistem IT de recunoaștere facială. Tehnologia este folosită deja de SRI', 19 September 2019, Hotnews, https://economie.hotnews.ro/stiri-telecom-23376576-politia-romana-incearca-din-nou-dezvolte-propriul-sistem-recunoastere-faciala-tehnologia-este-folosita-deja-sri.htm.

1254. Adrian Vasilache, 'Mai multe ONG-uri cer ca Poliția să renunțe la actuala achiziție a unui sistem IT de recunoaștere facială', 8 October 2019, Hotnews, https://economie.hotnews.ro/stiri-telecom-23412826-mai-multe-ong-uri-cer-politia-renunte-actuala-achizitie-unui-sistem-recunoastere-faciala.htm.

1255. Adrian Vasilache, 'Poliția Română încearcă, din nou, să-și dezvolte propriul sistem IT de recunoaștere facială. Tehnologia este folosită deja de SRI', already mentioned.

1256. Adrian Vasilache, 'Poliția Română va avea sistem IT de recunoaștere facială: Contractul a fost atribuit unei firme pentru 4,7 milioane de lei', 12 May 2020, Hotnews, https://economie.hotnews.ro/stiri-telecom-23990749-politia-romana-avea-sistem-recunoastere-faciala-contractul-fost-atribuit-unei-firme-pentru-4-7-milioane-lei.htm.

1257. Open letter from four civil society organisations to authorities, 8 October 2019, https://dpo-net.ro/wp-content/uploads/2019/10/OPEN-LETTER-implementing-the-facial-recognition-system.pdf (Romanian version: https://ascpd.ro/wp-content/uploads/2019/10/Scrisoare-Deschisa-sistem-recunoastere-faciala-final.pdf).

1258. Christiane Wendehorst and Yannic Duller, Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, August 2021, p. 17, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf. The report that presents the results of the experiment is available at this URL: https://www.europarl.europa.eu/RegData/questions/reponses_qe/2019/002653/P9_RE(2019)002653(ANN3)_XL.pdf.

1259. 'UTI to modernize video surveillance system of Bucharest's main airport', 6 May 2019, Romania Insider, https://www.romania-insider.com/uti-video-surveillance-otopeni-2019.

1260. As declared on the UTI website: https://www.uti.eu.com/about/history/.

1261. https://nordicunmanned.com/.

1262. Mike Ball, 'EMSA Surveillance UAV Deployed in Romania', 17 November 2020, https://www.unmannedsystemstechnology.com/2020/11/emsa-surveillance-uav-deployed-in-romania/. See also Nathan Gain, 'Romanian Border Police operating CAMCOPTER S-100 RPAS for maritime surveillance', 8 April 2021, https://www.navalnews.com/naval-news/2021/04/romanian-border-police-operating-camcopter-s-100-rpas-for-maritime-surveillance/.

1263. National Identification Number – Romania, https://www.liquisearch.com/national_identification_number/romania.

1264. Judice.ro, 'Critici la adresa proiectului SII Analytics. Reacția SRI. UPDATE: Finalizarea proiectului', 13 June 2019, https://www.juridice.ro/460184/critici-la-adresa-proiectului-sii-analytics.html. See also Sam Morgan, 'Romanian EU-funded project accused of data protection violations', 13 April 2017, https://www.euractiv.com/section/data-protection/news/romanian-eu-funded-project-accused-of-data-protection-violations/.

1265. Judice.ro, 'Critici la adresa proiectului SII Analytics. Reacția SRI. UPDATE: Finalizarea proiectului', already mentioned; Association for the Defense of Human Rights in Romania – the Helsinki Committee, 'Romanian Secret Service Gets €25 Million from EU for Mass Surveillance Project', 24 August 2016, https://www.liberties.eu/en/stories/romanian-secret-services-granted-european-fund-for-mass-surveillance/9555. In relation to original complaints, see Valentina Pavel, 'Sesizare către ANSPDCP: solicităm începerea unei investigații la toate instituțiile care au transmis date personale către SRI', 6 September 2016, https://www.apti.ro/sesizare-anspdcp-investigatie-transfer-date-personale-institutii-publice.

1266. The European Commission offered a very short and not very useful answer (ApTI, 'Comisia Europeană nu răspunde la sesizarea privind SII Analytics', 20 December 2016, https://apti.ro/raspunsul-ce-sesizare-sii-analytics). The Romanian DPA did not start investigations for national security reasons (Valentina Pavel, 'SII Analytics. Răspunsul Autorității pentru Protecția Datelor se ascunde după «securitatea națională»', 16 January 2017, https://www.apti.ro/raspuns-anspdcp-sii-analytics; Adrian Vasilache, 'SRI a copiat deja baze de date de la mai multe ministere si institutii cheie. Ce urmareste noul sistem IT de prevenire a fraudei, coruptiei, terorismului si evaziunii fiscale', 16 August 2016, HotNews.ro, http://economie.hotnews.ro/stiri-telecom-21229546-sri-copiat-deja-baze-date-mai-multe-ministere-institutii-cheie-urmareste-noul-sistem-prevenire-fraudei-coruptiei-terorismului-evaziunii-fiscale.htm). The OLAF's investigation did not find any irregularities. The Parliamentary Committee overseeing SRI's activity globally considered that the law was respected ('ApTI, Proiectul SII Analytics: Comisia de control a SRI ascultă SRI-ul, nu-l controlează', 14 April 2017, https://www.apti.ro/sii-analytics-raspuns-comisia-control-sri; Victoria Stoiciu, 'Comisia de control a SRI e de fapt portavocea SRI', 12 April 2017, http://www.romaniacurata.ro/comisia-

de-de-control-a-sri-e-de-fapt-portavocea-sri/).

1267. The SRI argued especially that, otherwise, the system "would not have been eligible for EU funds" (Translated from Romanian): Economica.net, 'SRI: SII Analytics nu amenin ă drepturile și libertă ile cetă enești, nu ar fi fost eligibil pentru fonduri UE', 12 August 2016, https://www.economica.net/sri-sii-analytics-nu-ameninta-drepturile-si-libertatile-cetatenesti-nu-ar-fi-fost-eligibil-pentru-fonduri-ue_123896.html.

1268. Economica.net, 'SRI: SII Analytics nu amenin ă drepturile și libertă ile cetă enești, nu ar fi fost eligibil pentru fonduri UE', already mentioned; Juridice.ro, 'Critici la adresa proiectului SII Analytics. Reacția SRI. UPDATE: Finalizarea proiectului', 13 June 2019, https://www.juridice.ro/460184/critici-la-adresa-proiectului-sii-analytics.html.

1269. It seems that the databases which were replicated by the SRI include the ones of the 9 following institutions: the Ministry of Internal Affairs, the Ministry of Finance with the Tax Authority (ANAF) and the Customs Office (ANV), the Ministry of Justice with the National Prison Office (ANP), the Ministry of Development (APIA) and the Agency for Financing Rural Investments (AFIR), the National Bank of Romania (BNR), the National Trade Register Office (ONRC) and the National Health Insurance House (CNAS). In addition, it is reported that the SII Infrastructure project might involve between 11 and 21 public institutions. See Adrian Vasilache, 'SRI a copiat deja baze de date de la mai multe ministere si institutii cheie. Ce urmareste noul sistem IT de prevenire a fraudei, coruptiei, terorismului si evaziunii fiscale', 16 August 2016, HotNews.ro, http://economie.hotnews.ro/stiri-telecom-21229546-sri-copiat-deja-baze-date-mai-multe-ministere-institutii-cheie-urmareste-noul-sistem-prevenire-fraudei-coruptiei-terorismului-evaziunii-fiscale.htm.

1270. Andrada Fiscutean, Romanian spies want to spot faces in a crowd - illegally, say human rights groups, 9 August 2016, https://www.zdnet.com/article/romanian-spies-want-to-spot-faces-in-a-crowd-illegally-say-human-rights-groups/.

1271. Juridice.ro, 'Critici la adresa proiectului SII Analytics. Reacția SRI. UPDATE: Finalizarea proiectului', already mentioned ; Valentina, 'Romanian Secret Services public statement confirms suspicions regarding mass surveillance', 9 August 2016, https://privacy.apti.ro/2016/08/09/romanian-secret-services-public-statement-confirms-suspicions-regarding-mass-surveillance/.

1272. Anca Bernovici, 'SIVECO to develop an IT system for SRI for EUR 20 M', 31 May 2017, Romania Journal, https://www.romaniajournal.ro/business/siveco-to-develop-an-it-system-for-sri-for-eur-20-m/.

1273. Adrian Vasilache, already mentioned.

1274. Translated from Romanian: Adrian Vasilache, afore-mentioned.

1275. Translated from Romanian: Adrian Vasilache, afore-mentioned.

1276. https://r-ss.ro/.

1277. http://azitrend.ro/.

1278. Asmag.com, 'TRASSIR ensures safety for Auchan hypermarkets in Romania', 27 September 2019, https://www.asmag.com/suppliers/pressreleases.aspx?co=trassir&id=3746 ; 'Security company in Romania uses TRASSIR to develop its security surveillance business', https://www.asmag.com/suppliers/pressreleases.aspx?co=trassir&id=3784.

1279. Asmag.com, 'TRASSIR provides security solutions for PROFI Romania', 7 November 2019, https://www.asmag.com/suppliers/pressreleases.aspx?co=trassir&id=3756.

1280. Asmag.com, 'TRASSIR provides security for AGRINVEST in Romania', 7 November 2019, https://www.asmag.com/suppliers/pressreleases.aspx?co=trassir&id=3761.

1281. Asmag.com, 'Security for ARABESQUE warehouses is powered by TRASSIR Neuro Detector', 27 September 2019, https://www.asmag.com/suppliers/pressreleases.aspx?co=trassir&id=3747.

1282. Asmag.com, 'New features in video analytics in TRASSIR 4 based on deep learning neural networks', 29 October 2018, https://www.asmag.com/suppliers/pressreleases.aspx?co=trassir&id=3635.

1283. Asmag.com, 'New features in video analytics in TRASSIR 4 based on deep learning neural networks', already mentioned.

1284. Roberta Kostadinova, 'Romania: Shaping digital future with new electronic ID cards', 4 August 2021, https://www.trendingtopics.eu/romania-shaping-digital-future-with-new-electronic-id-cards/.

1285. https://qoobiss.com/.

1286. Raluca Abrihan, 'Un sistem de plată prin recunoașterea facială creat de un startup românesc face parteneriat cu o companie de carduri de beneficii extrasalariale', 12 August 2020, https://www.startupcafe.ro/smart-tech/paybyface-card-tichete-recunoastere-faciala.htm.

1287. Luana Pascu, 'PayByFace launches biometric payments for Up Romania cardholders', 13 August 2020, BiometricUpdate.com, https://www.biometricupdate.com/202008/paybyface-launches-biometric-payments-for-up-romania-cardholders.

1288. Chris Burt, 'PayByFace launches touchless payments with facial biometrics to coffee chain in Romania', 24 July 2020, BiometricUpdate.com https://www.biometricupdate.com/202007/paybyface-launches-touchless-payments-with-facial-biometrics-to-coffee-chain-in-romania.

1289. Elena Ivanova, "Facial biometric payments startup PayByFace launches a pilot with one of the biggest banks in Bulgaria", 9 March 2021, Te Recursive, https://therecursive.com/facial-biometric-payments-startup-paybyface-launches-a-pilot-with-one-of-the-biggest-banks-in-bulgaria/.

1290. National Defence Strategy 2020-2024, esp. n° 59, https://www.presidency.ro/files/userfiles/National_Defence_Strategy_2020_2024.pdf; National Security Strategy 2007, especially p.37, https://www.bbn.gov.pl/ftp/dok/07/ROU_National_Security_Strategy_Romania_2007.pdf.

1291. Alexandra Sarc,inschi, 'Security perception and security policy in Romania, since the 1989 Revolution', 26 October 2020, in Defense & Security Analysis, 37, 2021, Issue 1, p.96-113 [p. 102], DOI:10.1080/14751798.2020.1831239, https://doi.org/10.1080/14751798.2020.1831239.

1292. Alexandra Sarcinschi, already mentioned, p. 108-109.

1293. China-cee Institute, 'The science and technology innovation mechanism of CEE countries. The case of Romania', 18 September 2020, https://china-cee.eu/2020/09/18/romania-economy-briefing-the-science-and-technology-innovation-mechanism-of-cee-countries-the-case-of-romania/.

1294. National Defence Strategy 2020-2024, already mentioned, n°51.

1295. See also, EDRI, 'Intelligence organisations get more surveillance powers in Romania', 6 April 2016, https://edri.org/our-work/intelligence-organisations-get-more-surveillance-powers-in-romania/.

1296. In 2014, a specialist wrote: "The political class wants more surveillance because more surveillance means more control and more control means more power; they use the terrorism excuse with abandon". Matei Vasile, '«Let's not talk about it»: how the mass surveillance debate was silenced in Romania', 27 May 2014, https://www.opendemocracy.net/en/can-europe-make-it/lets-not-talk-about-it-how-mass-surveillance-debate-was-silenced-in-/.

1297. OSAC, Romania 2020 Crime & Safety Report, 14 May 2020, https://www.osac.gov/Country/Romania/Content/Detail/Report/5fe2fbc7-a3e1-4ba4-833b-18af169bc1ec.

1298. Anne Hull, publication of a text from V. G. BALEANU, 'A clear and present danger to democracy: the new Romanian security services are still watching', https://irp.fas.org/world/romania/csrc12045.htm.

1299. European Commission, Commission Staff Working Document-Romania: Technical report, Accompanying document to the Report from the Commission to the European Parliament and the Council on Progress in Romania under the Cooperation and Verification Mechanism, COM(2019) 499 final, 22 October 2019, https://ec.europa.eu/info/sites/default/files/technical-report-romania-2019-swd-2019-393_0.pdf. The European Commission evokes amendments brought to three Justice laws in "a tense climate exacerbated by political criticism of the judiciary". Amended laws "could result in pressure on judges and prosecutors". Due to criticisms from the Commission, amended laws were suspended but emergency ordinances further modified the Justice laws, "without debate and consultation or ex-ante control […], sometimes modifying the same provisions repeatedly", thus affecting legal certainty and predictability.(p. 5). In relation to the content of amendments, they created "concerns about risks to judicial independence" (p. 6). Other amendments to the Criminal Procedure Code aimed at granting SRI with investigative powers, partly based on "cooperation protocols signed between the Public Ministry and the SRI", in a context where safeguards ensuring a proper supervision of SRI powers and the judicial independence appeared insufficient (p. 12-13).

1300. European Commission, Commission Staff Working Document-Romania: Technical report, already mentioned, p. 15-16.

1301. EDRI, 'The sixth attempt to introduce mandatory SIM registration in Romania', 23 October 2019, https://edri.org/our-work/the-sixth-attempt-to-introduce-mandatory-sim-registration-in-romania/; EDRI, 'Romania: Mandatory SIM registration declared unconstitutional, again', 26 February 2020, https://edri.org/our-work/romania-mandatory-sim-registration-declared-unconstitutional-again/.

1302. Translated from Romanian. Robert Mihailescu, 'Interviu HotNews.ro: Sebastian Ghita, deputat PSD -Vom depune o initiativa legislativa care sa permita interceptarea cartelelor telefonice pre-platite. Serviciile secrete trebuie sa dispuna de instrumente de tipul PRISM pentru supravegherea internetului in cazul terorismului si al infractiunilor economice', 17 July 2013, http://www.hotnews.ro/stiri-esential-15203892-sebastian-ghita-deputat-psd-vom-depune-initiativa-legislativa-care-permita-interceptarea-cartelelor-telefonice-pre-platite-serviciile-secrete-trebuie-dispuna-instrumente-tipul-prism-pentru-supravegher.htm.

1303. Matei Vasile, '"Let's not talk about it»: how the mass surveillance debate was silenced in Romania', 27 May 2014, https://www.opendemocracy.net/en/can-europe-make-it/lets-not-talk-about-it-how-mass-surveillance-debate-was-silenced-in-/.

1304. Chris Jones, 'National legal challenges to the Data Retention Directive', 8 April 2014, EU Law Analysis, https://eulawanalysis.blogspot.com/2014/04/national-legal-challenges-to-data.html.

1305. Romania Constitutional Court, Decision n° 1258 from 8 October 2009, http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf.

1306. EDRI, 'Romanian cybersecurity law sent to the Constitutional Court', 14 January 2015, https://edri.org/our-work/romanian-cybersecurity-law-sent-to-the-constitutional-court/; EDRI, 'Romanian cybersecurity law reloaded', 10 February 2016, https://edri.org/our-work/romanian-cybersecurity-law-reloaded/.

1307. https://selfd.id/.

1308. Alessandro Mascellino, 'Public service digital identity projects unveiled by Gradiant, ICI Bucharest and selfd.id', 19 February 2021, https://www.biometricupdate.com/202102/public-service-digital-identity-projects-unveiled-by-gradiant-ici-bucharest-and-selfd-id.

1309. See subsection 3.2 of the current study.

1310. Constitution of Romania republished, https://www.ccr.ro/wp-content/uploads/2020/11/constitutie-engleza.pdf; Cybercrime legislation, country profile – Romania, July 2016, https://rm.coe.int/090000168069d29f.

1311. Chart of signatures and ratifications of Treaty 005, Convention for the Protection of Human Rights and Fundamental Freedoms, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005?module=signatures-by-treaty&treatynum=005.

1312. Matei Vasile, '"Let's not talk about it»: how the mass surveillance debate was silenced in Romania', already mentioned.

1313. See above subsection 7.3.1.3 of the current study.

1314. EDRi, 'Icing on the cake: Romanian cybersecurity law unconstitutional', January 28, 2015 , https://edri.org/our-work/romanian-cybersecurity-law-declared-unconstitutional/.

1315. Law n° 190 of 18 July 2018, https://www.dataprotection.ro/servlet/ViewDocument?id=1520.

1316. Law n° 363 of 28 December 2018, https://www.dataprotection.ro/servlet/ViewDocument?id=1620.

1317. For example, the Authority sanctioned the processing

of employees' biometric data "for establishing the working hours and their video surveillance in the offices" and this sanction was confirmed by a Court: ANSPDCP, news, https://www.dataprotection.ro/index.jsp?page=Prelucrarea_datelor_biometrice_si_supravegherea_video_in_birourile_angajatilor_nelegale&lang=en. ANSPDCP also confirmed that failed a law that "provides adequate guarantees for the protection of data and the rights of data subjects, the purpose pursued does not justify" the "level of intrusion" constituted by the "processing of biometric data of visitors and employees" for accessing office premises: DLA Paper, 'Key aspects in the Romanian Data Protection Authority's annual activity report (2019)', 20 October 2020, https://www.lexology.com/library/detail.aspx?g=7b8ed9c6-86a1-4814-8d58-1cf8f5bafa72. The Autority also sanctioned a company for a lack of transparency in relation to CCTV video surveillance: Odia Kagan, 'Romanian Data Protection Authority Fines Company for Inadequate Notice of Video Surveillance', 6 August 2019, https://dataprivacy.foxrothschild.com/2019/08/articles/european-union/gdpr/romanian-data-protection-authority-fines-company-for-inadequate-notice-of-video-surveillance/;

1318. See especially the decision n° 52 of 31 May 2012, https://www.dataprotection.ro/servlet/ViewDocument?id=784.

1319. Valentina Pavel, 'SII Analytics. Răspunsul Autorității pentru Protecția Datelor se ascunde după «securitatea națională»', 16 January 2017, https://www.apti.ro/raspuns-anspdcp-sii-analytics.

1320. See subsection 7.3.1.2.1 of the current study.

1321. This answer was also provided by the ANSPDCP in its answer to the SII Analytics complaint. Government Decision n° 952/2003 refers to norms for operationalising the Integrated Information System, part of the National Electronic System.

1322. Law n° 51/1991 of 29 July 1991 - Law on the National Security of Romania, https://www.sri.ro/upload/law51.pdf.

1323. Matei Vasile, '"Let's not talk about it»: how the mass surveillance debate was silenced in Romania', 27 May 2014, https://www.opendemocracy.net/en/can-europe-make-it/lets-not-talk-about-it-how-mass-surveillance-debate-was-silenced-in-/; Valentina, 'Romanian Secret Services public statement confirms suspicions regarding mass surveillance', 9 August 2016, https://privacy.apti.ro/2016/08/09/romanian-secret-services-public-statement-confirms-suspicions-regarding-mass-surveillance/.

1324. Anne Hull, publication of a text from V. G. BALEANU, 'A clear and present danger to democracy: the new Romanian security services are still watching', https://irp.fas.org/world/romania/csrc12045.htm.

1325. See above, subsection 7.3.6.1 of the current study.

1326. See subsection 4.1 of the current study.

1327. Judice.ro, 'Critici la adresa proiectului SII Analytics. Reacția SRI. UPDATE: Finalizarea proiectului', 13 June 2019, https://www.juridice.ro/460184/critici-la-adresa-proiectului-sii-analytics.html.

1328. In 2016, the NGO ApTI asked the ANSPDCP to start an investigation relating to the public authorities that provide the SRI with their database within the framework of the SSI Analytics system. No investigation was opened, but the ANSPDCP answered that it notified the public authorities. See Valentina Pavel, 'Sesizare către ANSPDCP: solicităm începerea unei investigații la toate instituțiile care au transmis date personale către SRI', 6 September 2016, ApTI, https://www.apti.ro/sesizare-anspdcp-investigatie-transfer-date-personale-institutii-publice.

1329. https://www.apti.ro/sesizare-anspdcp-investigatie-transfer-date-personale-institutii-publice.

1330. Public authority may establish sharing protocols, but these are generally not announced publicly. As a result, it is very difficult to know what kind of data sharing mechanisms are in place.

1331. CJEU, 3rd ch., 1 October 2015, Smaranda Bara and Others, case C-201/14, https://curia.europa.eu/juris/document/document.jsf?docid=168943&doclang=EN.

1332. For example, APTI (https://apti.ro/) and the Association for the Defense of Human Rights in Romania (https://www.liberties.eu/en/about/our-network/the-association-for-the-defense-of-human-rights-in-romania-the-helsinki-committee) are active in the field and have raised awareness on challenges posed by several legislative proposals.

1333. Example of Judice.ro, which proposed a summary relating to the debates that surrounded the SII Analytics project. See 'Critici la adresa proiectului SII Analytics. Reacția SRI. UPDATE: Finalizarea proiectului', 13 June 2019, https://www.juridice.ro/460184/critici-la-adresa-proiectului-sii-analytics.html.

1334. See for example V. M., 'Protest in Capitala impotriva «Legilor Supravegherii»', 12 July 2014, https://www.hotnews.ro/stiri-esential-17660968-protest-capitala-impotriva-legilor-supravegherii.htm.

1335. Alexandra Sarcinschi, 'Security perception and security policy in Romania, since the 1989 Revolution', 26 October 2020, in Defense & Security Analysis, 37, 2021, Issue 1, p. 96-113, DOI:10.1080/14751798.2020.1831239, https://doi.org/10.1080/14751798.2020.1831239.

1336. Mihai Sebe, 'Soul search, national and European identity and politics in a time of trouble', March 2016, Building Bridges Paper Series, p. 4, https://www.ifri.org/sites/default/files/atoms/files/sebe_-_soul_search_national_and_european_politics.pdf. The author observes that despite "Romania has always been a Europhile country […], the Romanian public has not been subjected to much information regarding the European Union, which is often coloured by politicians' views".

1337. Mihai Sebe, 'Soul search, national and European identity and politics in a time of trouble', already mentioned, p. 4.

1338. Mihai Sebe, 'Soul search, national and European identity and politics in a time of trouble', already mentioned, p. 4.

1339. Dumitrita Holdis, Media influence matrix: Romania, CEU's Center for Media, Data and Society (CMDS), Budapest, 2019, P.5, https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/basicpage/1509/mimromaniatech.pdf.

1340. Matei Vasile, '«Let's not talk about it»: how the mass surveillance debate was silenced in Romania', 27 May 2014, https://www.opendemocracy.net/en/can-europe-make-it/lets-not-talk-about-it-how-mass-surveillance-debate-was-silenced-in-/.

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[1340] 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.

[1340] *Michel Benichou, 'Le résistible déclin du secret', LPA, 20 June 2001, n° 122, p. 3 s.*

9

ANNEX 1

LACK OF LEGITIMATE BASIS OF LEGAL INSTRUMENTS THAT ORGANISE THE POSSIBILITY OFMASS BIOMETRIC RECOGNITION

9.1 ABSENCE OF LEGITIMATE LEGAL BASIS OF THE EU REGULATION 2019/1157 ON STRENGTHENING THE SECURITY OF IDENTITY CARDS

EU Regulation 2019/1157 on strengthening the security of identity cards is based on article 211341 of the Treaty on the Functioning of the European Union (TFEU)[1342]. Article 21 1 grants EU citizens the *"right to move and reside freely within the territory of the member states"*. Article 21 2 states that *"If action by the Union should prove necessary to attain this objective and the Treaties have not provided the necessary powers, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may adopt provisions with a view to facilitating the exercise of the rights referred to in paragraph* 1*"*. Article 1 3 states that *"for the same purposes as those referred to in paragraph* 1 *and if the Treaties have not provided the necessary powers, the Council, acting in accordance with a special legislative procedure, may adopt measures concerning social security or social protection. The Council shall act unanimously after consulting the European Parliament."*

As a result, the proposal for Regulation 2019/1157 explains that it *"aims to facilitate the exercise of the right to free movement of EU citizens in a secure environment, i.e. to facilitate their right to travel to and reside in any Member State with their national identity cards and to rely on these cards there as reliable proof of nationality, as well as their right to rely on the residence documentation issued to them as residents of a Member State other than their country of nationality."* This proposal further explains that *"Article* 21*(2) TFEU expressly provides a legal basis for measures to facilitate the exercise of free movement of EU citizens, including by reducing the risk of fraud in the form of forgery of documents and by ensuring the trust needed for free movement"* and that the proposal *"will provide for more secure documents, through improved security features of national identity cards and residence documents, which will allow exercising free movement rights in a more secure environment. This will protect public authorities and EU citizens and their family members from crime, falsification and document fraud. Accordingly, this proposal contributes to improving the overall security within the EU"*.

However, article 21 2 only provides the European Parliament and the Council with legislative powers in case their action is *"proven necessary […] with a view to facilitating the exercise of the rights of free move and residence"*. The European Union did not demonstrate that the general collection of facial images and fingerprints of all the EU citizens and residents, whether in a chip or in a database[1343], is *"necessary"* to a freedom of movement and residence that was already effective beforehand. They also did not demonstrate that this collection is *"necessary"* to reduce a risk of fraud that would, otherwise, prejudice the freedom of movement.

As a result, this legal basis does not appear to be legitimate. Moreover, this issue is visible in the explanatory statement itself, which seems like an exercise in semantics that desperately tries to justify a link between the TFUE and proposed measures[1344].

9.2 ABSENCE OF LEGITIMATE LEGAL BASIS FOR A PROPOSED ARTIFICIAL INTELLIGENCE REGULATION

The proposal for a regulation on artificial intelligence is based on article 114 TFUE[1345], which grants the European Parliament and the Council with the power to *"adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market"* for the achievement of *"the objectives set out in Article* 26*"*, which in turn further defines the notion of internal market. Therefore, the proposal for a regulation states that its primary objective *"is to ensure the proper functioning of the internal market by setting harmonised rules"* in the area of AI, addressing *"the situation after AI systems have been placed on the market by harmonising the way in which ex-post controls are conducted"*.

However, the authorisation given to member states to use biometric technologies in public areas is not covered by the regulation and the functioning of the internal market. The proposal for a regulation on AI has therefore no legal basis in this respect.

In addition, the explanatory statements for the proposal for a regulation base this regulation on article 16 of the TFUE, which grants the European Parliament and the Council with the power to lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the member states. Article 16 clarifies that *"compliance with these rules shall be subject to the control of independent authorities"*.

However, as pointed out by the EDPB and the EDPS in their joint opinion relating to this proposal for a regulation, *"article* 16 *TFEU provides an appropriate legal basis in cases where the protection of personal data is one of the essential aims or components of the rules adopted by the EU legislature"*[1346], which is not the case of the proposal, taking into account that the GDPR and the Police-Justice Directive do actually already constitute a legal framework for the protection of personal data.

Moreover, in relation to the use by law enforcement agencies of AI systems for 'real time' or post remote biometric identification in publicly accessible spaces, in addition to the very limited prohibition of artificial intelligence practices set-up in article 5 1 of the proposed Artificial Intelligence Act, the latter act does not, actually, organise the protection of personal data, but, on the contratry, it organises the possibility to use artificial intelligence technologies which pose high risks to freedoms, including the possibility to massively monitor the population for law enforcement purposes, whereas, currently, no legal basis enables such operations unless the provisions of the GDPR or the Police-Justice Directive are respected, including a specific legal basis for law enforcement processing.

Finally, as also pointed out by the EDPB and the EDPS in their joint opinion, *"the application of Article* 16 *TFEU also entails the need to ensure independent oversight for compliance with the requirements regarding the processing of personal data, as is also required Article* 8 *of the Charter of the Fundamental Rights of the EU"*[1347]. On this aspect the proposed Artificial Intelligence Act does only provide for a judicial supervisory obligation for 'real-time' remote biometric identification in publicly accessible space for LE purposes, but not in the other situations. Further, the proposal does not clarify that rules relating to the use of AI technologies are subjected to *"the application of existing EU laws governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments"*[1348].

As a consequence, the legal bases invoked to legitimate the proposal for an artificial intelligence act do not enable setting-up provisions that, in

practice and under the guise of prohibiting the use of certain technologies, actually authorise the use of other high risk technologies including the use of 'real time' and post remote biometric identification in publicly accessible space for LE purposes, without framing them by the necessary safeguards that would drive to ascertain that fundamental rights are appropriately respected. In case a proper fundamental rights assessment would fail to demonstrate the necessity and proportionality of the interference, such safeguards should basically be summarised in a general prohibition to use biometric technologies on individuals in public places, which meets the conclusions of the EDPB and EDPS joint opinion in relation to *"any use of AI for an automated recognition of human features in publicly accessible spaces - such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals - in any context"*[1349].

1341. Proposal for a Regulation of the European Parliament and of the Council on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement, COM/2018/212 final - 2018/0104 (COD), n° 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0212

1342. Consolidated version of the treaty on the functioning of the European Union, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_2&format=PDF.

1343. The legislation has the perverse effect of organising the technical possibility for all member states to collect and retain those data. See subsection 5.2 of the current study.

1344. See also Statewatch, 'EU: Biometrics - from visas to passports to ID cards', https://www.statewatch.org/media/documents/analyses/no-49-eu-bio-passports-id-cards.pdf. This publication raises similar concerns in relation to article 18 of the TFEU which based the proposal for this regulation.

1345. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final, n° 2.1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

1346. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), p. 2 and n° 11 p. 7, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

1347. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), already mentioned, p. 2. See also n°11.

1348. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), already mentioned, n°15.

1349. EDPB – EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), already mentioned, p°2.

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