Global Campus Europe

KU Leuven
Faculty of Law

European Master's Programme in Human Rights and Democratisation
A.Y. 2019/2020

Framing the picture: A human rights-based study on AI, the case of Facial Recognition Technology

Author: Francesco Paolo Levantino
Supervisors: Prof. Koen Lemmens and Mr. Jonas Vernimmen

ABSTRACT

From science-fiction novels and dystopian literary scenarios, Artificial Intelligence (AI) has become a distinguishing feature of our times. AI-based technologies have the potential to decrease the mortality caused by car accidents or serious diseases, and the detrimental effects of climate change. Yet, all that glisters is not gold. We live surrounded by security cameras, unconsciously caught by the lens of private smartphones, dashcams integrated into vehicles, and regularly overflow by drones and orbiting satellites. Among these various forms of surveillance, Facial Recognition Technology (FRT) plays a central role. The present thesis aims at investigating, analysing and discussing several threats FRT can pose to human rights, democracy and the rule of law. To do so, its uses by law enforcement authorities will be "framed" adopting the European human rights law framework. This research will unveil that the risks connected to the deployment of FRT are increased when advocated for the pursuit of "public security". Based on the performed analysis, it can be concluded that, whilst proper regulations would mitigate the adverse effects generated by FRT, the general public should be more sensitive to data protection and privacy issues in order to enable an environment for "human flourishing".

TABLE OF ABBREVIATIONS

AI	Artificial Intelligence
CCTV	Closed-circuit Television
CFR	Charter of Fundamental Rights of the European Union
CJEU	European Court of Justice
CoE	Council of Europe
CRPD	Convention on the Rights of Persons with Disabilities
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
FRA	European Union Agency for Fundamental Rights
FRSs	Facial Recognition Systems
FRT	Facial Recognition Technology
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ICESCR	International Covenant on Economic Social and Cultural Rights

IoT	Internet of Things
ITU	International Telecommunication Union
LED	Law Enforcement Directive
ODIHR	Office for Democratic Institutions and Human Rights
OSCE	Organization for Security and Co-operation in Europe
R&D	Research and Development
SDGs	Sustainable Development Goals
TFEU	Treaty on the Functioning of the European Union
TEU	Treaty on European Union
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
US	United States of America

Table of Contents

Introduction

From science-fiction novels and dystopian literary scenarios, Artificial Intelligence (AI) has become a distinguishing feature of our times. The very term itself, referring to computer systems able to achieve pre-set goals by reproducing human cognitive abilities,[1] is now part of everyday life. In a hyper-connected world, whereby technological devices can interact with each other, and where every element of reality is "measurable" and "data-translatable", AI emerges as one of those technologies '*blurring the boundaries between human and machine, between online and offline activities, between the physical and the virtual world, between the natural and the artificial, and between reality and virtuality*'.[2]

Beyond the most trivial examples involving the use of smartphones, virtual assistants, and "apps", AI is able to power aeroplane navigation systems, thus limiting the pilots' intervention to only a few flight phases.[3] Similar systems are being developed in the field of self-driving cars, and recent applications of AI in healthcare sound extremely promising.[4] Also, the analysis of large amounts of data – which constitute the "food" through which AI is able to work – has been used in clinical research to predict psychosis, suicidal ideation, or self-harm.[5] Yet, the specific use of AI in mental health assessments reveals a lot about the hidden risks of AI in general.

---

[1] *Infra*, Chapter I. AI and fundamental rights, an overview.; *1.2 How can 'something' be intelligent? A working definition of AI.*

[2] Council of Europe, PACE Recommendation, *Technological convergence, artificial intelligence and human rights*, 28 Apr. 2017, 2102(2017).

[3] '*Everyday Examples of Artificial Intelligence and Machine Learning'*, emerj The AI Research and Advisory Company, 10 Mar. 2020, available at *https://emerj.com/ai-sector-overviews/everyday-examples-of-ai*.

[4] Amnesty International & Access Now, *The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems.*, 2018, available at https://www.torontodeclaration.org/declaration-text/english/. See also Taddeo M. & Floridi L., *How AI can be a force for good, Science*, 361(6404), 2018, 751-752.

[5] Corsico P., *The risks of risk. Regulating the use of machine learning for psychosis prediction*, International journal of law and psychiatry, 66, 101479, 2019.

Indeed, the possibility to entrust data-driven decision-making processes with such relevant implications for someone's life may lead to '*the paradoxical effect of harming the individual while trying to prevent harm*'.[6]

Precisely this kind of reflections seem equally applicable to all those areas where the use of AI by public authorities, for the prevention of social harm and the maintenance of social order, can strongly affect individual rights, democracy, and the rule of law.

As its title intends to suggest, the present research aims at investigating, under a human rights perspective, the implications of AI as an extraordinary and multifaceted technology of the contemporary world. Delving deep into this topic, the research will focus on one of its most topical utilisations, namely Facial Recognition Technology (FRT). To provide an idea about the importance of examining this type of AI-powered system, it is useful to remind that it has played a relevant role in two main events which have characterised 2020 so far. That is, FRT has been used by certain States to detect and track 'COVID-19 quarantine evaders',[7] as well as it has been deployed among the surveillance tools used by law enforcement to identify and monitor protestors during the demonstrations following George Floyd's death in May.[8]

At first glance, such measures may appear as justified responses to current extraordinary situations; on the one hand, the urgent need to reverse the trend of a global pandemic, on the other hand, state reactions to the violent escalation of peaceful demonstrations against the abuse in the use force by law enforcement. Yet, to discover which issues the deployment of FRT systems may give rise to, even in the counteraction to public health and security crises, it is essential to better define the

---

[6] *Ibid.*, 6.

[7] Oliver K. & Neenan A., *In the blink of AI: How facial recognition technology is capitalising on the COVID-19 crisis*, Euronews, 14 May, 2020, available at https://www.euronews.com/2020/05/14/in-the-blink-of-ai-how-facial-recognition-technology-capitalising-on-covid-19-crisis-view; Habersetzer N., Moscow Silently Expands Surveillance of Citizens, Human Rights Watch, 25 March 2020, available at https://www.hrw.org/news/2020/03/25/moscow-silently-expands-surveillance-citizens.

[8] Schoolov K., *How police use powerful surveillance tech to track George Floyd protests*, CNBC, 18 June 2020, available at https://www.cnbc.com/2020/06/18/heres-how-police-use-powerful-surveillance-tech-to-track-protestors.html.

concept of AI and to understand how – in the different shapes it can take – this technology intersects with democracy and human rights. This objective will be pursued within Chapter I of the present thesis. Additionally, before introducing how facial recognition works, which tasks it can perform, how it can be used by law enforcement, and which impact such uses may have on specific sets of fundamental rights, it is necessary to specify the standpoint from which this analysis will be conducted. Subsequently, this constitutes one of the main focuses of Chapter II.

After 9/11, the fear generated by an increase in terrorist acts threatening liberal democracies' model of life has been the *rationale* for the public acceptance of intensified uses of surveillance. To a certain extent, since the early 21st century, ordinary citizens unconsciously surrendered fragments of their freedoms for supposedly higher levels of protection guaranteed through intrusive forms of surveillance and social control.[9] As a matter of perception, such practices went mostly unnoticed in our daily lives because not immediately evident to the general public which, nowadays, is increasingly familiar – with forms of *surveillance capitalism*[10] – *e.g.*, through the use of social media. That is why these methods should be considered as extremely insidious.[11]

Against this background, the protection from serious crimes and threats to the Western model of life should not be ensured through sharp trade-offs between the pursuit of security and the respect for fundamental rights, as the use of powers

[9] Barnard-Wills D. & Wells H., *Surveillance, technology and the everyday*, in Criminology & Criminal Justice, 12(3), 2012, 227-237, 229; Marcella A. J. & Stucki C., *Privacy Handbook: Guidelines, Exposures, Policy Implementation and International Issues*, Hoboken, NJ: John Wiley & Sons, 2003, 12.

[10] Zuboff S., *Big other: surveillance capitalism and the prospects of an information civilization*, Journal of Information Technology, 30(1), 2015, 75-89. By the same author, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books, 2019.

[11] Sarre R., Brooks D., Smith C. & Draper R., *Current and emerging technologies employed to abate crime and to promote security*, in Arrigo B., & Bersot H. (Eds.), *The Routledge handbook of international crime and justice studies*, Routledge, 2013, 328. '*Surveillance today is so pervasive, and has so many dimensions, that it has simply become part of everyday life*', in these terms Bauman Z., Bigo D., Esteves P., Guild E., Jabri V., Lyon D. & Walker R. B., A*fter Snowden: Rethinking the impact of surveillance* in International political sociology, 8(2), 2014, 121-144, 142, refer to the current *familiarity* of surveillance.

'*especially liable to abuse […] risks to destroy democracy "on the ground of defending it"*'.[12] Eventually, the cyclical recurrence of 'new crises' to be countered with exceptional measures may generate pathological frictions with the basis of every democratic system and the essence of free societies.[13]

It would be both reductive and incorrect to picture democracy as the mere rule of a nation through representatives elected by universal suffrage. Rather, democratic values materialise through the respect of human rights for each individual as '*the core of substantive democracy*'. [14] In the same way, a substantive and not just formal conception of the rule of law is particularly recurrent in the influential case-law of both the European Court of Justice (CJEU) and the European Court of Human Rights (ECtHR).[15]

Within this context, the European systems of fundamental rights protection – encompassing EU law, the Charter of Fundamental Rights (CFR), and the European Convention on Human Rights (ECHR)[16] – can serve as a reference to 'frame', under a human rights perspective, the uses of FRT by law enforcement. Although the far-reaching repercussions such uses may give rise to,[17] the present study is limited to the "surveillance dimension" of this technology, which will be here analysed through the rights to privacy, data protection, and peaceful assembly. However, as it will become clearer in due course, throughout this paper several reflections will touch upon the right

[12] De Vries K., *Right to Respect for Private and Family Life*, in van Dijk P., van Hoof F., van Rijn A., Zwaak L. (Eds), *Theory and Practice of the European Convention on Human Rights*, 5th Ed., Intersentia, 2018, 672.

[13] Extensively on these themes, Greene A., *Permanent States of Emergency and the Rule of Law: Constitutions in an Age of Crisis*. Bloomsbury Publishing, 2018.

[14] On the distinction between "formal" and "substantive" democracy, Barak A., *A Judge on Judging: The Role of a Supreme Court in a Democracy*, Harvard Law Review, 116(1), 2002, 19-162, 20.

[15] *Communication from the Commission to the European Parliament and the Council, A new EU Framework to strengthen the Rule of Law*, 11 Mar. 2014, COM(2014) 158 final, and note 11 therein.

[16] On this notion of *European human rights law*, Malgieri, G., & De Hert, P., *European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably But Not Necessarily by Judges*, Cambridge Handbook of Surveillance Law, 2017, 509-532, 510.

[17] *i.a.* European Union Agency for Fundamental Rights (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019.

to a fair trial and the impact of law enforcement uses of FRT on the rule of law. This last element will also be the object of the final chapter of this dissertation, namely Chapter III.

For practical reasons, the scope of this research is limited to law enforcement activities related to crime control and criminal investigations. Despite the study of the increasingly blurred boundaries between intelligence agencies, the military and law enforcement powers[18] is certainly an interesting field, additional considerations make it particularly intricate to deepen within the limited space of this composition. Indeed, the analysis of this subject would imply a more extensive discussion about the concept of "national security". Moreover, according to Articles 4(2) TEU and 72 TFEU, the processing of data for national security purposes '*falls out of the scope of the EU treaties*',[19] thus excluding any relevance of the provisions on the processing of personal data by law enforcement authorities set out in Directive 2016/680.[20] By contrast, the reference to the EU data protection framework will be a key element of this analysis.

However, considerations about surveillance activities conducted by intelligence services will not be completely excluded from this human rights-based study on FRT. As underlined by the European Parliament in its resolution of 12th March 2014, '*Member States must fully respect EU law and the ECHR while acting to ensure their national security*'.[21] From this perspective, an overview of relevant case-law about

[18] Malgieri, G. *et al*., *supra* note 16, 519; Casagran C. R., *Surveillance in the European Union*, in Gray D., & Henderson S. E. (Eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge University Press 2017, 654.

[19] *Ibid.*, 654. Cf. Arts. 4(2) TEU and 72 TFUE.

[20] Art. 2. 3(a) and Recital (14) '*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*'

[21] Caruana M. M., *The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement*, International Review of Law, Computers & Technology, 33(3), 2019, 249-270, 256. See also European Parliament, Resolution 12 March 2014, *on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* (2013/2188(INI) [P7_TA(2014)0230].

surveillance will be useful in reconstructing the theoretical framework regarding the particular protection offered under the European human rights law to the list of selected rights.

Methodology

In conducting the present desk research, a legal approach has been predominantly adopted. The legal perspective will hopefully be easily recognisable, as it will make direct use of the primary sources and relevant case-law each time indicated. However, to properly "frame" the variety of issues that the contemporary intersection among human rights, modern technologies, and surveillance gives rise to, it is fundamental to critical assess several points by integrating elements from other social sciences, *i.a.* surveillance studies. This multi-disciplinary approach is reflected by the broad variety of sources interrogated. Taking into account the extremely dynamic nature of the research topic, which can be described as a "fast-moving target", an extensive literature review showed the lack of up-to-date leading publications on the subject matter. Hence, it has been necessary to reconstruct a consistent theoretical framework by combining (1) doctrinal sources as academic papers, journals, books, and commentaries with (2) grey literature, including working papers, white papers, technical or research reports from academia, research centres, governmental, non-governmental and inter-governmental entities. To maintain the research in line with the latest developments, render the idea of the extremely topical nature of the subject matter, and describe the practical social implication the use of FRT can have in our society, this study also makes extensive use of press articles and recent news.

The structure follows a progressive course, which sees certain reflections gradually being integrated with further elements emerging during the discussion. In this view, some arguments will be recurrently recalled, others will be assumed to be constantly present as part of the conceptual background of this composition. Due to a similar construction, a composite analysis of the topics covered will take place throughout the text. Therefore, the final remarks of this paper will only consist of some reflections emerged thanks to this research.

CHAPTER I.

AI and fundamental rights, an overview.

1. These are times for AI. A brief Introduction.

1.1 AI as a composite reality.

What would your answer be if someone asked you "How frequently do you meet with AI in your daily life?". If you think this question is purely rhetorical, as your answer would simply be "every day", it is probably because the use of technological systems operating through the schemes of Artificial Intelligence (AI) is already inextricably entrenched in various spheres of our life.

AI is no longer a futuristic concept borrowed from the universe of science fiction; yet – in its different shapes – AI is embedded in everything around us.[22] An idea of this can be rendered if we consider the intertwining of the 'Internet of Things' (IoT) with the domains of health monitoring, wearable technology, home automation along with many other applications[23] part of the 'datafication' process of our lives and reality.[24]

---

[22] In this sense, Communication from the Commission to the European Parliament, the European Council, the Council, the European economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, 24 Apr. 2018, COM(2018) 237 final; Raso F. A., Hilligoss H., Krishnamurthy V., Bavitz C. & Kim L., *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center Research Publication, (2018-6), 2018, 7.

[23] Generally, IoT indicates the possibility of "smart devices" to interact, connect and communicate through data, hence offering users personalised experiences. "Smart devices" are those able to adapt their performances to different circumstances thanks to the gathering and analysis of data. See Friedland S. I., *The Internet of Things and Self- Surveillance Systems*, in Gray D. *et al.*, *supra* note 18, 199-223; van Est R., Gerritsen J. B. A. & Kool L., *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality*, Expert report for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE), Rathenau Institute, 2017; Girasa R., *Artificial Intelligence as a Disruptive Technology*, Palgrave Macmillan, 2020, 147-150.

[24] *i.a.* Mayer-Schönberger V. & Cukier K., *Big data: A revolution that will transform how we live, work. In and Think*, John Murray Publishers Ltd London, 2013, 78.

Such an *AI environment* encompasses numerous technological niches and sub-branches.[25] Each of those can, in turn, be applied to perform specific functions.[26] In this sense, AI is one of those *suitcase notions*[27] so wide to frame a broad range of nuances. This versatility in applications and variety of purposes might be the result of the impressive growth this field has experienced throughout its history, that – surprisingly – is not as recent as it could be generally imagined.

Whilst the notion of AI would intuitively recall the activities this technology commonly allows us to perform with personal devices – like finding the most convenient route to reach an unknown destination or get musical recommendations based on our preferences[28] – to consider AI a brand-new concept would be a mistake. This term was conceived in 1956 by the computer scientist McCarthy at the first academic conference in this field.[29] Therefore, the lack of a generally accepted or agreed definition of AI is rather surprising.

Indeed, the evolution of this technology in terms of capabilities and applications and the increasing number of professionals from different backgrounds interested in

[25] '*it is useful to think of "AI" as a catchphrase for a cluster of technologies embedded in social systems. This includes machine learning, natural language processing, computer vision, neural networks, deep learning, big data analytics, predictive models, algorithms, and robotics.*', see Latonero M., *Governing artificial intelligence: Upholding human rights & dignity*, Data & Society, 2018, 8. See also Girasa, R., *supra* note 23, 13-22.

[26] Legrain P. and Lee-Makiyama H. compare AI to '*steam, electricity or computing […] general-purpose technology with a wide range of applications*' in *Ever Clever Union How AI could help EU institutions become more capable, competent, cost-effective and closer to citizens*, Open, 2019, 37.

[27] Winston P.H., *Self-Aware Problem Solving*, Computational models of Human Intelligence Community, Report Number 2, 2018. The latter referring to Minsky M., *The Society of Mind*, Simon and Schuster, 1988; *The Emotion Machine*, Simon and Schuster, 2006.

[28] For further '*Everyday Examples of Artificial Intelligence and Machine Learning',* emerj, *supra* note 3.

[29] McCarthy J., Minsky M. L., Rochester N. & Shannon C. E., *A proposal for the Dartmouth summer research project on artificial intelligence*, 1955, in AI magazine, 27(4), 2006, 12. See also Smith C., McGuire B., Huang T. & Yang G., *The history of artificial intelligence*, University of Washington, 2006, 27; Elish M. C. & Boyd D., *Situating methods in the magic of Big Data and AI*, Communication monographs, 85(1), 2018, 57-80. About the inconsistency between the emergence of AI and the rise of public attention on the theme, see Calo R., *Artificial intelligence policy: primer and roadmap*, U.C. Davis Law Review, 51(2), 2017, 399-436, 401. See also Girasa, R., *supra* note 23, 6-8.

it,[30] resulted in many definitions of AI. Each one mirrors the specific approach adopted in that particular area of study.[31]

In such a dynamic environment, since this research aims at understanding how certain uses of AI can adversely impact on fundamental rights, it is essential to set as a common ground a working definition of AI.

1.2 How can "something" be intelligent? A working definition of AI.

For the purposes of this paper, to answer the question "What is AI?" it will be sufficient to combine the literal meaning of this expression with a few technical connotations. In doing so, we will refer to influential definitions of AI available in different sources.

First of all, the concept of *intelligence* can be outlined as a capacity referable to sentient creatures. Indeed, animals and human beings are able to perceive a surrounding environment through the senses and interact with it according to their needs. Thus, artificially intelligent are all those '*scientific methods, theories and techniques whose aim is to reproduce […] the cognitive abilities of human beings*'.[32]

The fact that the replication of 'human cognitive abilities' is performed by computer systems[33] that '*sense, reason, learn, act and adapt much like humans do*'[34]

---

[30] The scientific roots of AI can be found in '*Computer Science, Philosophy, Mathematics, Psychology, Cognitive Science and many other disciplines.*', see Dignum V., *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*. Springer International Publishing, 2019, 11; Tecuci G., *Artificial Intelligence*, WIREs Comput Stat, 4/2012, 168-180.

[31] Girasa R., *supra* note 23, 7-10; Villani C., *For a Meaningful Artificial Intelligence towards a French and European Strategy*, 2018, 4, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf.

[32] European Commission for the Effectiveness of Justice (CEPEJ), *European ethical Charter on the use of Artificial Intelligence in Judicial Systems and their environment*, Council of Europe, 2018, 69.

[33] AI is described as '*a form of "intelligent computing*"' by Manheim K. & Kaplan L., *Artificial Intelligence: Risks to Privacy and Democracy*, Yale Journal of Law & Technology, 21(1), 2019, 106-189, 113.

[34] *Ibid.*, 113. Similarly McCarthy J., *What Is AI? / Basic Questions*, in Jmc.Stanford.Edu. 2018, available at http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html.

by '*collecting and interpreting data, reasoning on what is perceived or processing the information derived from this data*'[35] constitutes the *artificiality* of such forms of intelligence.

Thereby, AI can be framed as the category including those techniques or mechanisms allowing computer systems the accomplishment of certain goals, through the simulation of human cognitive processes like perceiving surroundings, learning, and making decisions.[36]

One of the most astonishing features characterising some of these systems is the ability to learn by gathering and analysing the data attained through their "experiences". This ability of AI to modify its functioning[37] using 'human rational processes'[38] was presented just as a '*higher level of abstraction*' until a few decades ago.[39] Nowadays, instead, the capability to learn and adapt improving performances through the acquisition of experience, the interactivity with the surroundings in terms of input/output, and the forms of autonomous agency, are three essential features of AI.[40]

Having just touched upon this few entry points on the complex world of AI,[41] and being aware of the myriad of nuances in terminology, technicalities, and

---

[35] High-Level Expert Group on Artificial Intelligence established by the European Commission, *A definition of AI: Main Capabilities and Disciplines*, 8 Apr. 2019, 1.

[36] Similarly, the Montréal Declaration for a Responsible Development of Artificial Intelligence, Université de Montréal, 2018, available at https://5dcfa4bd-f73a-4de5-94d8c010ee777609.filesusr.com/ugd/ebc3a3_5c89e007e0de440097cef36dcd69c7b0.pdf. See also Dignum V., *supra* note 30, 9-34.

[37] '*Machine learning systems are set a task, and given a large amount of data to use as examples of how this task can be achieved or from which to detect patterns. The system then learns how best to achieve the desired output.*', see Royal Society Working Group (GB), *Machine learning: the power and promise of computers that learn by example*, Technical report, 2017, 19.

[38] High-Level Expert Group on Artificial Intelligence established by the European Commission, *supra* note 14, 1.

[39] Samuel A. L., *Some Moral and Technical Consequences of Automation – A Refutation*, Science 132(3429), 1960, 741-742.

[40] Taddeo M. *et al*., *supra* note 4; Floridi L. & Sanders J. W., *On the morality of artificial agents*, Minds and machines, 14(3), 2004, 349-379.

[41] On the relationship among the three key concepts of *AI*, *Machine Learning* and *Deep Learning* see the short clip by Intel News, *Artificial Intelligence Explained: Unleashing the Next Wave*, Nov. 2016, available at https://youtu.be/vehXkgG3YcU.

applications excluded here because beyond the scope of this composition, we will now introduce the different roles AI can play in the context of human rights and democracy. As these seemingly distant spheres are instead strictly connected.

2. AI in the context, human rights and democracy.

2.1 Intersections, AI and human rights.

Once a working definition of AI is set, and its essential features highlighted, it is time to contextualise, from a human rights perspective, its impact on the contemporary reality, with a few relevant examples.

The current state-of-the-art of such technologies is certainly not limited to the smartphone's applications in daily use. For instance, AI-based technologies are helping humanitarian organisations to detect and take action in areas severely affected by natural disasters, armed conflicts, poverty and health emergencies.[42] In Africa, the use of AI tools supports in addressing the lack of medical care access suffered by rural or remote communities.[43] What is more, the use of AI in the agricultural sector appears extremely promising, since it significantly improves both the quality and quantity of food production.[44]

Other AI-based technologies have the great potential to decrease the mortality caused by car accidents,[45] by certain serious diseases, or by the detrimental effects of

[42] *e.g.* Jean N., Burke M., Xie M., Davis W. M., Lobell D. B. & Ermon S., *Combining satellite imagery and machine learning to predict poverty*, Science (80-.)353, 2016, 790-794.

[43] Besaw C. & Filitz J., *Artificial Intelligence in Africa is a Double-edged Sword*, United Nations University (Centre for Policy Research), Jan. 16 2019, available at https://ourworld.unu.edu/en/ai-in-africa-is-a-double-edged-sword.

[44] See *How AI Can Improve Agriculture for Better Food Security***,** AI for Good - Global Summit 28-31 May 2019, International Telecommunication Union (ITU-UN), available at https://itu.foleon.com/itu/aiforgood2019/ai-and-agriculture/.

[45] Report from the Commission to the European Parliament and the Council, *Saving Lives: Boosting Car Safety in the* EU, 12 Dec. 2016, COM(2016)787 final.

climate change,[46] thanks to self-driven cars, diagnostic instruments[47] and other tech-tools.

From a human rights perspective, these few examples already show how AI is having a positive impact in achieving many of the seventeen Sustainable Development Goals (SDGs) adopted in 2015 by the UN General Assembly, as objectives of the 2030 Agenda for Sustainable Development.[48] Among others, the targets most positively affected appear those related to the fight against poverty, the field of human health and well-being, the access and quality of education, and the environmental sustainability.[49]

Yet, the other side of the coin shows how AI can as well hinder the realisation of other SDGs or part of them.[50] For instance, let us consider another area of great

[46] The '*mitigation of the adverse effects of climate change*' is among the positive impacts of AI mentioned in recent communications by the European Commission. See, COM(2018)237 final and COM(2020)65 final.

[47] *Ibid*. The helpfulness of AI in diagnostic medicine and for the accessibility of healthcare services is stressed as well in *The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems, supra* note 4. See also Taddeo M. *et al.*, *supra* note 4.

[48] A recent study extensively analysed both positive and negative repercussions of AI on the realisation of the SDGs (2015). See Vinuesa R., Azizpour H., Leite I., *et al.*, *The role of artificial intelligence in achieving the Sustainable Development Goals*, Nature Communications 11, 2020. About the link between new technologies and the achievement of the SDGs, also, Guterres A., *UN Secretary-General's Strategy on New Technologies*, United Nations, September, 2018 available at https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf; Trudy J., *Governing Artificial Intelligence to benefit the UN Sustainable Development Goals*, Sustainable Development, 2020, 1–14. Further examples of helpful/harmful AI with regard to human rights can be found in the report by Access now, *Human rights in the age of artificial intelligence*, 2018, 14-16; Land M. K. & Aronson J. D., *The Promise and Peril of Human Rights Technology*, in New Technologies for Human Rights Law and Practice, Cambridge University Press, 2018, 1-20.

[49] To exemplify the magnitude of such an impact, here some of the human rights each of those objectives encompasses: the right to an adequate standard of living (UDHR art. 25; ICESCR art. 11); right to adequate food (UDHR art. 25; ICESCR art. 11); right to life (UDHR art. 3; ICCPR art. 6); right to health (UDHR art. 25; ICESCR art. 12); right to enjoy the benefits of scientific progress and its application (UDHR art. 27; ICESCR art. 15(1)(b)); right to education (UDHR art. 26; ICESCR art. 13). See https://www.ohchr.org/Documents/Issues/MDGs/Post2015/SDG_HR_Table.pdf .

[50] '*Each application of AI impacts a multitude of rights in complicated and, occasionally, contradictory ways*' in Raso F. *et al*., *supra* note 22, 4; Vinuesa R. *et al*. *supra* note 48. Some of the '*challenges from Existing and Near-Term Capabilities*' of AI are listed in Kemp L. *et al*., *UN High-level Panel on Digital Cooperation: A Proposal for International AI Governance*,

social importance, as the social care for the elderly and the disabled. Here, the use of technologies has significantly enhanced the quality and quantity of the support provided, consequently intensifying the empowerment,[51] advancement and enjoyment of fundamental human rights by the beneficiaries of these services. In such areas, the deployment of AI brings great advantages in terms of effectiveness and timesaving, as it allows caregivers to commit themselves to those activities that require the most direct human agency.[52] Despite that, all that glisters is not gold; eventually, similar assistive technologies could actually impact on the human dignity of their care receivers by generating adverse effects such as device-dependence, loss of social skills, and autonomy.[53]

On a global scale, another area generating significant concern regards AI-based weaponry. Whilst, the use of autonomous weapons might reduce the number of human casualties in armed conflicts, especially considering those killings induced by instinctive emotions like fear or anger; on the other hand, the same emotional deficiency also implies the lack of genuine "lifesaving" sentiments as empathy or compassion. One day, these devastating devices could end up in the armoury of dangerous non-state actors or terrorist groups; also, authoritarian leaders could extend their use in intrusive activities of social control, hence generating further threats to fundamental rights and freedoms.[54]

2019. See also Brundage M. *et al*., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Technical Report, 2018.

[51] See *e.g.* the commitments on 'AI for accessibility', respectively by Microsoft and Apple, available at https://www.microsoft.com/en-us/ai/ai-foraccessibility?SilentAuth=1&wa=wsignin1.0 ; https://www.apple.com/accessibility/.

[52] Kornfeld-Matte R., *Report of the Independent Expert on the enjoyment of all human rights by older persons*, United Nations Doc. A/HRC/36/48, 2017.

[53] Whilst the protection of human dignity can be intended as the ultimate foundation of every human right, the independence and autonomy of persons with disabilities are values characterising the Convention on the Rights of Persons with Disabilities (CRPD), United Nations General Assembly RES/61/106, 2007.

[54] Future of Life Institute, *Autonomous weapons: An open letter from AI & robotics researchers*, 2015, available at https://futureoflife.org/open-letter-autonomous-weapons/; Docherty B. L., *Shaking the foundations: The human rights implications of killer robots*, Human Rights Watch, 2014, 6; Heyns C., *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, United Nations Doc. A/HRC/23/47, 2013.

In any case, even if we were to disregard the mentioned adverse impacts of AI on human rights, further reflections relate to the inequality in access to beneficial technological applications. Indeed, not only the purchase by private individuals, but also research, development, and production of the most advanced AI-based technologies, involve considerable investment. If we consider the already high level of inequalities characterising our world,[55] the lack of resources impinging on the equal access to AI-based technologies could further exacerbate inequalities among individuals, states, and regions of the world.

At this point, even without digging down into details, the ubiquitous impact of AI on human rights should have already emerged; therefore, the intersection of AI with the very core of every democratic society will now be considered.

2.2 Intersections, AI and democracy.

Although AI can impact on democratic foundations in ways much wider than one could intuitively expect, today the most immediate concerns for the quality of Western democracies involve the weaponised use of AI to manipulate the outcome of democratic elections.[56]

Similar uses of digital warfare in political campaigns threat the authentic core of every open society, namely the active participation of citizens in the government of their country through '*the free expression'* of their will in '*periodic and genuine elections*'.[57] In this context, two clear examples of dangerous (mis)uses of AI are the

[55] According to Oxfam, the 1% of the global population holds 50% of the world wealth. See Hardoon D., *An economy for the 99%*, Oxfam Policy Papers, 2017.

[56] For the use of AI, machine learning, big data and other technologies in '*political warfare*' see Polyakova A. & Boyer S. P., *The future of political warfare: Russia, the West, and the coming age of global digital competition*, Brookings Robert Bosch Foundation - Transatlantic Initiative, 2018.

[57] That is the right to free elections as enshrined in Art. 21 UDHR, United Nations General Assembly Resolution 217 A, 1948; in Art. 25 ICCPR, adopted and opened for signature, ratification and accession by the UN General Assembly with Resolution 2200A XXI, 1966; and at the regional level, in Art. 3, 1st Additional Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, ECHR, 1952.

result of the 'Brexit' *referendum* for the withdrawal of the UK from the EU in 2016, and the outcome of the 58th presidential elections in the US. Indeed, both these events have been found to be significantly influenced by targeted campaigns aimed at persuading the vote of those electors easier to manipulate.[58] Such *computational propaganda campaigns*,[59] relied on the massive spread of fake news,[60] on the use of psychometrics, and sentiment analysis.

Psychometrics is the measurement of people's personality through the data extracted from online behaviours and activities,[61] while sentiment analysis is an investigation of the voters' emotional attitude deduced from portions of text available on social media.[62] Accordingly – as in the case of political campaigns managed by Cambridge Analytica – AI was used by candidates and political parties to harness voters' *digital personalities*, strategically influencing their electoral choices.[63]

---

[58] '*Recent research suggests that elections may be won not by the candidates with the best political argument, but by those who use the most efficient technology to manipulate voters, sometimes emotionally and irrationally*' see Wagner B., *Algorithms and Human Rights, study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, Committee of experts on internet intermediaries (MSI-NET), 2016, 30; Woolley S. C., & Howard P., *Computational propaganda worldwide: Executive summary*, Computational Propaganda Research Project, Working Paper No. 2017.11, Oxford University, 2017, 7; Polyakova A. *et al*., *supra* note 56, 10-12; Polonski V., *How artificial intelligence silently took over democracy*, Word Economic Forum, 9 Aug. 2017, available at https://www.weforum.org/agenda/2017/08/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first.

[59] Involving the '*use of algorithms, [and] automation […] to purposefully distribute misleading information over social media networks.*', see Woolley S. C. *et al*., *supra* note 58, 3.

[60] The expression *fake news* '*refers to news that is verifiably false that is intentionally placed in various forms of written communication using recognized news and social media outlets particularly that of newspapers and Facebook*' see Girasa, R., *supra* note 23, 212.

[61] About its use by the company Cambridge Analytica see Stanley J., *Meet Cambridge Analytica: the Big Data communications company responsible for Trump & Brexit*, 2 Feb. 2017, available at https://nota-uk.org/2017/02/02/meet-cambridge-analytica-the-big-data-communications-company-responsible-for-trump-brexit .

[62] Practice also called *opinion mining*, see Bannister K., *Understanding Sentiment Analysis: What It Is & Why It's Used*, 26 Feb. 2018, available at https://www.brandwatch.com/blog/understanding-sentiment-analysis .

[63] Taddeo M. *et al*., *supra* note 4.

Malicious contents, once shared among virtual "circles of friends", spread on a massive scale as in virtual echo chambers reaching exponential levels of diffusion.[64] Within this framework, fake social-media accounts powered by forms of '*conversational AI*', which are capable of autonomously create and share preposterous contents and "comments", also play a significant role.[65] Yet, the rapid development of more and more performing digital technologies fueled by AI is significantly improving the possibility to forge video or audio contents with results so realistic to render the detection of these manipulations extremely hard.[66]

Against this background, it will not be difficult to imagine the use of these techniques to create '*synthetic multimedia'*.[67] Similar *'hyper-realistic digital falsification[s]'*[68] could be an unpredictable instrument if in the wrong hands of illiberal or authoritarian regimes. Especially in countries with limited access to independent media, it would be easy to get rid of political opponents, activists, and investigative journalists using AI to frame them as terrorists or dangerous criminals with fabricated evidence. What is more, in a world increasingly prone to violence, artificial contents could be powerfully leveraged by non-state actors or foreign intelligence services for incitement towards internal or external conflicts.[69]

---

[64] Kramer A. D., Guillory J. E., & Hancock J. T., *Experimental evidence of massive-scale emotional contagion through social networks*, Proceedings of the National Academy of Sciences, 111(24), 2014, 8788-8790.

[65] To know more about these practices and the counter-actions adopted by certain social networks, see Acker A., *Tracking Disinformation by Reading Metadata*, Medium, 17Jul. 2018, available at https://medium.com/@MediaManipulation/tracking-disinformation-by-reading-metadata-320ece1ae79b.

[66] Chesney B. & Citron D., *Deep fakes: A looming challenge for privacy, democracy, and national security*, Calif. L. Rev., 107, 2019, 1753-1820, 1759.

[67] Brundage M. *et al*, *supra* note 50, 46.

[68] Chesney B. *et al.*, *supra* note 66, 1757.

[69] On the use of fake audio and video contents '*in the realms of politics and international affairs*' see Chesney R. & Citron D., *Deepfakes and the new disinformation war: The coming age of post-truth geopolitics*, Foreign Affairs, 98(1), 147-155. On such forms of '*psychological warfare*' see Pantserev K.A., *The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability*, in Jahankhani H., Kendzierskyj S., Chelvachandran N., Ibarra J. (Eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Springer, 2020, 37-55.

In these circumstances, the use of social media psychological manipulations and *deep fakes*[70] to influence the results of 'free and fair' elections, repress dissidents, or destabilise fragile democracies, appears of great concern. Particularly when operated by actors external to the domestic political framework,[71] similar practices deem in contrast with democratic principles and could be interpreted in light of Article 1 of the UN Charter which – mindful of colonial experiences and aggressive territorial conquests – erects the relations among nations on the principle of self-determination of peoples.[72]

3. The governance of emerging technologies. Conclusions.

To condemn technology for the highly controversial and alarming uses shown above would be simplistic. Indeed, '*technology is neither good nor bad; nor is neutral*'[73] and only those benefiting from its harmful effects on democratic systems should be held accountable. Yet, certain adverse effects of modern technologies might be mitigated by developing adequate legislative frameworks to regulate the design and use of such technologies in ways compatible with human rights, democracy and the rule of law.[74]

Currently, every level of the global legal community is engaging in discussions and public consultations about the most appropriate way to regulate AI[75] in order to

[70] Pantserev K.A., *supra* note 69, 39.

[71] *e.g.* Polyakova A. *et al*., *supra* note 56; Girasa, R., *supra* note 23, 212-215.

[72] United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI.

[73] Kranzberg M., *Technology and History:" Kranzberg's Laws"*, Technology and culture, 27(3), 1986, 544-560, 545.

[74] These three elements have been labelled as the 'trinitarian formula' of liberal constitutionalism by Kumm M., *The cosmopolitan turn in constitutionalism: an integrated conception of public law*, Indiana J Global Legal Studies 2013, cited in Nemitz P., *Constitutional democracy and technology in the age of artificial intelligence*, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2018. They are also '*interdependent'* and in a '*mutually reinforcing*' relationship see Res. *Human Rights, democracy and the rule of law*, United Nations Doc. A/HRC/RES/28/14, 2015.

[75] Among numerous initiatives see *The AI for Good Global Summit*, the leading UN platform for global and inclusive dialogue on AI. For a comprehensive list of the different

enhance its beneficial applications, while preventing the erosion of the fundamental values our democracies are based on.[76]

However, the intersection among democracy, human rights and technological developments is not a recent one. On the contrary, in May 1968 the final act of the first UN international conference on human rights[77] already stressed the sound capabilities of technological applications in fostering the effective achievement of human rights.

On the same occasion, it was emphasised that technological developments

> '*may entail certain dangers for the rights of the individual or of the group and for human dignity and that, in any event, their utilization raises complex, ethical and legal problems with respect to human rights*'.[78]

With all this in mind, at least three of the four recommendations issued by the International Conference in that very moment are still relevant today. These are (1) the necessity of pursuing constant interdisciplinary researches in order to formulate adequate standards; (2) the urgency to attain '*respect for privacy in the view of recording techniques*'; (3) and lastly the importance to investigate '*the use of electronics which may affect the rights of the persons and the limits which should be placed on its uses in a democratic society*', '*more generally, the [necessity of a] balance between scientific and technological progress and the intellectual, spiritual, cultural and moral advancement of humanity*'. Accordingly, in 1975 the UN General Assembly followed these considerations with the 'Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind;[79] its 2nd Paragraph particularly stresses the urgency *to take*

initiatives about AI operated under the UN umbrella see *United Nations Activities on Artificial Intelligence (AI)*, International Telecommunication Union (ITU UN), 2019.

[76] At the regional level these values can be effectively summarised in terms of 'European values' as enshrined in Article 2 TEU, but also in the CFR, in the ECHR or in the preamble of the Statute of the CoE of 1949.

[77] See paragraph 18 of the Proclamation of Teheran and Resolution XI.

[78] See Final Act of the International Conference on Human Rights, Teheran, 22 April to 13 May 1968, United Nations Doc. A/CONF. 32/41, 1968.

[79] See, UNGA Res. 3384 (XXX), 10 November 1975.

> *appropriate measures to prevent the use of scientific and technological developments, particularly by the State organs, to limit or interfere with the enjoyment of the human rights and fundamental freedoms of the individual as enshrined in the Universal Declaration of Human Rights, the International Covenants on Human Rights and other relevant international instruments*.

Still today, the challenge is to gather together all the different stakeholders coming from the governmental, non-governmental, inter-governmental and private sector to favour the intertwining of AI with our lives as a generator of virtuous circles instead of vicious ones.[80]

In the light of these principles, and of the complex scenario briefly drawn above, the attention will be now specifically focused on some critical issues concerning the deployment of AI for crucial state functions, and its possible impact on different, universally protected, human rights and fundamental freedoms.

[80] '*Learning to Live with Artificial Intelligence: "A Virtuous Circle or a Vicious One?*"', International Peace Institute, 22 Jun. 2018, available at https://www.ipinst.org/2018/06/governing-artificial-intelligence#5.

CHAPTER II.

The dangerous gaze of AI. The use of Facial Recognition Technology in law enforcement, a fundamental rights perspective.

1. Setting the scene.

1.1 AI, security and surveillance.

Since 09/11 many governmental agendas have been dominated by political discourses focused on national security.[81] The chain reaction thus initiated shifted the balance among different public interests at the expenses of fundamental rights and civil liberties.[82]

In this context, the *unprecedented* nature of new forms of international terrorism[83] opened the route to *exceptional* measures including '*the use of torture, inhuman and degrading treatment at the detention facilities located in Guantanamo Bay, […] "black sites" used for interrogation, extended state surveillance powers, and the use of biometric data in the regular practices of States'*.[84]

As far as these practices are concerned, it can be observed how from 2001 to date, particularly those measures entailing surveillance and the use of biometrics have far from disappeared. On the contrary, phenomena of collection, storage and analysis

[81] About this concept, see Wolfers A., *"National security" as an ambiguous symbol*, Political science quarterly, 67(4), 1952, 481-502; Baldwin D. A., *The concept of security*, in Review of International Studies, 23(1), 1997, 5-26; Rothschild E., *"What Is Security?"*, Daedalus 124(3), 1995, 53-98; Scott, P. F., *The National Security Constitution*. Bloomsbury Publishing, 2018; Goold B. J. & Lazarus L. (Eds.), *Security and Human Rights*, Bloomsbury Publishing, 2019.

[82] On the potential of the concept of 'security' Baldwin D. A., see *supra* note 81, '*security is an important concept, which has been used to justify suspending civil liberties, making war, and massively reallocating resources*', 9.

[83] In UNSC Res. 2322 (2016) the Security Council declared all '*forms and manifestations*' of terrorism as '*one of the most serious threats to peace and security*', United Nations Doc. S/RES/2322, 2016.

[84] Aolain F., *How can states counter terrorism while protecting human rights*, Ohio Northern University Law Review, 45(2), 2019, 389-410; Gearty C., *Terrorism and human rights*, Government and Opposition, 42(3), 2007, 340-362.

of personal data have extensively risen in intensity, while keeping up with technological innovation.[85]

Although at first glance these events had a greater impact in the US, both terroristic attacks[86] and intrusive surveillance practices also significantly involved the EU and its citizens.[87]

In this regard, Snowden's revelations in 2013 opened a breach in the opaque curtains covering the pursuing of national security through highly intrusive exercises of state powers.[88] However, the apprehension due to the risk of the "next attack", made *extraordinary* measures generally well-accepted among highly intimidated societies, which have been even supportive of their implementation.[89]

Thus, over time, the transitory shift in the prioritisation of societal and constitutional values has progressively assumed a permanent place in the collective

[85] Gray D. *et al.*, *supra* note 18.

[86] On most recent terroristic attacks occurred within the EU see, *Terrorism in the EU: terror attacks, deaths and arrests*, published on 6th Sep, 2019, available at https://www.europarl.europa.eu/news/en/headlines/security/20180703STO07125/terrorism-in-the-eu-terror-attacks-deaths-and-arrests.

[87] '*The PRISM case to a large extent involves direct US access to Europeans' […] personal data that is stored and processed in the US due to the technical infrastructure of the internet and because many major internet services […] are US-based.*', see Joergensen R. F., *Can human rights law bend mass surveillance?*, Internet Policy Review 3(1), 2014, 1-9, 5. In addition, according to Casagran C. R. *'many studies have concluded that Internet surveillance programmes in the European Union are equivalent to those of the NSA.*', in *Surveillance in the European Union*, Gray D. *et al.*, *supra* note 18, 643-658, 642. See also the European Parliament LIBE and JHA Committee Report, 21 Feb. 2014 [A7-0139/2014] and the following EP resolutions of 12th Mar. 2014 [P7_TA(2014)0230], 29 Oct. 2015 [P8_TA(2015)0388]. Within the context of the CoE similarly Resolution 2045(2015) adopted by the PACE on 21st Apr. 2015 following the report about mass surveillance of the Committee on Legal Affairs and Human Rights, AS/Jur (2015) 01.

[88] About the extensive use of mass surveillance by the US National Security Agency (NSA) and other law enforcement agencies, see *i.a.* the interactive report of The Guardian, NSA FILES: DECODED, 1 Nov. 2013, available at https://www.theguardian.com/us-news/the-nsa-files. For a broader analysis Bauman Z. *et al.*, *supra* note 11; Levinson-Waldman R., *NSA Surveillance in the War on Terror*, in Gray D., *supra* note 18, 7-43.

[89] A survey conducted shortly after 9/11 depicted 86% of Americans 'in favour to an increment in the use of Facial Recognition Technology', see Marcella A. J. *et al.*, *supra* note 9, XIX. See also Sulowski S., *Counter-Terrorism: Correlating Security and Freedom*, in Sroka A., Castro-Rial Garrone F., and Torres Kumbrián R. D. *Radicalism and Terrorism in the 21st Century*, Peter Lang AG, 2017, 11-23.

routine.[90] The exceptional nature of counter-terrorism measures has been degraded into "normality" and the acquiescence to the *rituals of security*[91] makes phenomena as mass surveillance '*emerging as a dangerous habit rather than an exceptional measure'*.[92] In this framework, mass surveillance can be defined as any form of monitoring conducted towards a vast array of individuals without a pre-existent identified suspicion.[93]

The adoption of such Western pre-emptive attitudes towards security[94] seriously affected also the sphere of criminal justice and its tenets.[95] Indeed, the purpose of eliminating the occurrence of the next aggression somehow softened the sharp distinction between law enforcement and intelligence activities, their corresponding competencies, and practices.[96] Hence, reactive approaches towards

[90] *e.g.* Hernandez R., *Surveillance by default: PATRIOT Act extended?*, EDRi – European Digital rights, 1 April 2020, available at https://edri.org/surveillance-by-default-patriot-act-extended; Lyon D., *Surveillance Society,* Talk for Festival del Diritto, Piacenza, Italia, 2008.

[91] An example of those rituals is the "traveller's experience", who to reach a destination undergoes luggage scans and checks, inspections, various identification processes – including biometrics. See also New York Post, *JFK Airport's Terminal 1 launches facial recognition boarding*, 8 Oct. 2019, available at https://nypost.com/2019/10/08/jfk-airports-terminal-1-launches-facial-recognition-boarding/. Such experiences can be tougher for certain "high-risk" travellers as suggested by Goold B. J., *Trusted Travellers and Trojan Horses: Security, Privacy, and Privilege at the Border*, in Goold B. J. *et al.*, *supra* note 81, 125-144.

[92] OHCHR Report, *The right to privacy in the digital age*, United Nations Doc. A/HRC/27/37, 2014. Of the same opinion Barnard-Wills D. *et al.*, *supra* note 9.

[93] Jakubowska E. & Naranjo D., *Ban Biometric Mass Surveillance A set of fundamental rights demands for the European Commission and EU Member States*, EDRi, - European Digital Rights, 13 May 2020, 10, available at https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf.

[94] Pavone V., Santiago Gomez E., & Jaquet-Chifelle D. O., *A systemic approach to security: beyond the tradeoff between security and liberty*, in Democracy and Security, 12(4), 2016, 225-246.

[95] In this sense '*the post-crime orientation of criminal justice is increasingly overshadowed by the pre-crime logic of security*', see Zedner L., *Pre-crime and post-criminology?*, Theoretical criminology, 11(2), 2007, 261-281. Extensively on this topic Wilson D. & McCulloch J., *Pre-crime: Pre-emption, precaution and the future*, Routledge, 2017; Gray D. *et al*., *supra* note 18, 122-149, 149; Vervaele, J. A., *Surveillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system?*, in Reloading Data Protection, Springer, 2014, 115-128.

[96] Bauman Z. *et al*., *supra* note 11, 125; Sulowski S., *supra* note 89, 19.

already committed offences turned into preventive policing actions before *potential risks* turn in actual *harm*.[97]

Against this background, crimes may *probably* be concealed in the "normality" of a simple behaviour, of a gait. Consequently, it becomes indispensable to gather as much information as possible to permit – in the Big Data era[98] – the analysis and sorting of human behaviours to anticipate "the next strike". In doing so, the steady monitoring becomes a crucial method to protect from a harm that could have never happened.[99] In this respect, the use of AI assumes an essential role in the performance of all those investigative practices implemented through data mining,[100] profiling,[101] tracking,[102]

[97] Barnard-Wills D., supra note 9. '*Surveillance measures are now woven into the fabric of everyday life […]*' write Haggerty K. D., Wilson D. &. Smith G. J, in *Theorizing surveillance in crime control,* Theoretical criminology, 15(3), 2011, 231-237; Wilson D. *et al*., see *supra* note 95, 3.

[98] Big Data is '*Datasets that are too large or complex for traditional data processing software to analyze.'* furthermore, *'The increasing availability of big data, thanks to society's ever-expanding internet use, and coupled with rapid improvements in computing power, has enabled the significant advances in AI in the past 10 years.*' see Access Now, *supra* note 48, 8. See also Ferguson A. G., *Big Data Surveillance: The Convergence of Big Data and Law Enforcement,* in Gray D. *et al*., *supra* note 18, 171-197.

[99] Barnard-Wills D., *supra* note 9, 230. See also Lippens R. & Gardiner-Bess R., *Technologies of crime control: international developments and contexts*, in Arrigo B., *supra* note 11, 350-370, 357.

[100] Data mining is '*[t]he process of discovering patterns and extracting information from large datasets. In the era of big data, data mining is often facilitated by machine learning [a sub-field of AI]*' see Access Now, *supra* note 48, 8. The process of '*building a mathematical model to make predictions based on input*' is also referred to as *predictive analytics.* See Perry W. L., McInnis B., Price C., Smith S. C., and Hollywood J. S., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation, 2013, 35.

[101] Thus, referring to '*the systematic and purposeful recording and classification of data related to individuals—a profile is thus a compilation of data referring to an individual.*' See Büchi M., Fosch-Villaronga E., Lutz C., Tamò-Larrieux A., Velidi S. & Viljoen S., *The chilling effects of algorithmic profiling: Mapping the issues*, Computer Law & Security Review, 2020. The European General Data Protection Regulation (GDPR) defines profiling in Article 4(4) as '*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*'. See also European Union Agency for Fundamental Rights (FRA), *Preventing unlawful profiling today and in the future: a guide*, 2018.

[102] About this practice where '*some entity changes state, [and] a computer internally represents those states, and certain technical and social means are provided for […] maintaining the correspondence between representation and the reality.*', see Agre P.E.,

mapping, tapping, *et cetera*.[103]

Within this scenario, the old-fashioned paradigm of a detective working on a notebook full of handwritten notes and engaged in scrutinising post-crime gathered evidence seem to be fading forever.[104]

To date, although forms of dataveillance[105] do not imply direct and physical observations anymore, the visual nature of traditional forms of surveillance and social control still maintain a central relevance.[106] We live surrounded by CCTV systems and ATM security cameras, we are unconsciously caught by the lens of private smartphones and dashcams integrated into vehicles, we are regularly overflow by drones and orbiting satellites.[107]

Facial Recognition Technology (FRT) has recently joined this category. Yet, due to its operating modes, which will be analysed shortly, the use of this technology involves the regulation of data protection, in particular of biometrics, and that is not all. Indeed, the risks related to the increasingly widespread use of intrusive video surveillance may lead to '*a [dangerous] change in cultural norms leading to the acceptance of lack of privacy as the general outset*'.[108]

Surveillance and capture: Two models of privacy, The information society, 10(2), 1994, 101-127; see also Pell S. K., *Location Tracking*, in Gray D. *et al*., *supra* note 18, 44-70.

[103] Sarre R., *supra* note 11; Raaijmakers S., *Artificial Intelligence for Law Enforcement: Challenges and Opportunities*, IEEE Security & Privacy, 17(5), 74-77, 2019.

[104] Similarly, Haggerty K. D. *et al*., see *supra* note 68. See also Wilson D. *et al*., see *supra* note 95, 7.

[105] *i.a* Clarke R., *Information technology and dataveillance*, Communications of the ACM, 31(5), 1988, 498-512.

[106] Marx, G. T., *What's New About the "New Surveillance"? Classifying for Change and Continuity*, Surveillance & Society, 1(1), 2002, 9-29.

[107] Cf. Introna L. & Wood D., *Picturing algorithmic surveillance: The politics of facial recognition systems*, Surveillance & Society, 2(2/3), 177-198, 181.

[108] European Data Protection Board (EDPB), *Guidelines 3/2019 on processing of personal data through video devices*, 2019, 5.

1.2 Facial recognition is the gaze of AI.

In Chapter I, AI has been described as an extraordinary technology able to perform a vast array of applications in many different fields. Howbeit, its current level of development does not allow a single artificial agent to execute all the tasks human beings can generally perform.

While the just mentioned system would commonly fall within the category of *general* or *strong AI*, the type of AI currently available is defined as *narrow* or *weak AI*. Indeed, such expression indicates systems specifically designed to perform one or a limited number of well-determined tasks.[109]

Facial recognition technology (FRT) or facial recognition systems (FRSs) are specific applications of narrow AI in the field of computer vision.[110] In a few words, such *'detection technologies'*[111] can identify human faces through their characteristic facial traits.[112] However, the way such machines perceive faces is not comparable to the kind of perception a person would have. In fact, if it is true that also human agents use innate forms of facial recognition to identify other human beings, FRSs identify our distinctive traits as a *'set of discernible pixel-level patterns'*.[113] In this sense, systems operating through geometry feature-based algorithms code into a '*mathematical representation*'[114] the geometric relationships among key facial traits as

[109] *A definition of AI*, *supra* note 35, 5; Access Now, *supra* note 48, 8.

[110] Girasa R., *supra* note 23, 18.

[111] Faggella D., *AI and Machine Vision for Law Enforcement – Use-Cases and Policy Implications*, emerj The AI Research and Advisory Company, 20 May 2019, available at https://emerj.com/ethics-and-regulatory/ai-and-machine-vision-for-law-enforcement-use-cases-and-policy-implications/.

[112] For accessible descriptions on 'how does FRT works' see *i.a.* Lynch J., *Face Off Law Enforcement use of facial recognition technology*, Electronic Frontier Foundation (EFF), 2020, 4-6; Introna L. & Nissenbaum H., *Facial recognition technology a survey of policy and implementation issues*, Working Paper 2010/030, Lancaster University Management School, 2010, 10-11; THALES, *Facial recognition: top 7 trends*, 16 Feb. 2020, available at https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition.

[113] See Introna L. *et al.*, *supra* note 107, 186.

[114] See Lynch J., *supra* note 112, 5. The same mathematical representation of facial features is defined as '*mathematical artifact*' in Introna L. *et al.*, *supra* note 107, 9 or as '*facial signature*' see Martin N., *The Major Concerns Around Facial Recognition Technology*, Forbes, 25 Sep. 2019, available at https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-

'*the distance between the eyes, width of the nose, and the depth of the eye sockets'*.[115]

Even in this instance, considering the vast amount of different definitions and technicalities available, it is essential to use a working definition of FRT. Therefore, we will adopt the definition elaborated by the Data Protection Working Party[116] referring to FRT as '*the automatic processing of digital images which contain the faces of individuals for [1] identification, [2] authentication/verification or [3] categorisation of those individuals*'.[117]

In the following pages, each of these three functions will be essentially described in their technical properties. Afterwards, those same functions will be contextualised thanks to some case studies related to their existing and near future uses by law enforcement. Hereinafter, we will indicate law enforcement authorities in line with the definition provided by Article 1(1) of the EU 'Law Enforcement Directive' (LED), which refers to them as the State '*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*'.[118]

The selected episodes – which mainly take place in the European Union (EU) and in the United States of America (US) – will be analysed through the lens of the European human rights law framework as it will be further described in the following

---

concerns-around-facial-recognition-technology/. For an outline of the different steps characterising the work of FRSs see Davies B., Innes M. and Dawson A., *An evaluation of South Wales police's use of Automated Facial Recognition*, Universities' Police Science Institute Crime & Security Research Institute, Cardiff University, 2018, 11. For an overview on such systems see Zahid M., Nazeer M., Nargis B., Tauseef A., *A Review on state-of-the-art face recognition approaches*, Fractals, 25(2) 2017.

[115] This kind of algorithms *'often locate anchor points at key facial features (eyes, nose, mouth, etc), connect these points to form a net and then measure the distances and angles of the net to create a unique face "print"*', see Introna L. *et al.*, *supra* note 107, 185. For the list is quotes see *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, Nlets – the International Justice and Public Safety Network, 2011, 9.

[116] Independent European advisory body with competence on data protection and privacy, today replaced by the European Data Protection Board.

[117] Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192*, 22 Mar. 2012, 2.

[118] Art. 1 and Recital (11) LED.

section. This approach will allow addressing the impressive capabilities of FRSs while critically assessing the fluid intersection among human rights, surveillance, and modern technologies.

2. Human Rights Protection in Europe.

2.1 The European Human Rights Law Framework.

Before analysing from a human rights perspective how the deployment of FRT by law enforcement can negatively impact upon civil rights, such as the right to the protection of personal data, the right to privacy and the right to freedom of assembly, it appears appropriate to briefly specify the theoretical legal framework that will be utilised in such an assessment.[119]

Within the EU, the right to respect for private life is enshrined in Article 7 of the Charter of Fundamental Rights of the European Union (CFR), whilst the protection of personal data is therein protected as a fundamental right under Article 8(1).[120] The system of data protection law is then more specifically regulated through the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) which applies as *lex specialis* to the processing of personal data 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*'.[121]

At the regional level, thanks to the case-law of the European Court of Human Rights (ECtHR) both these mentioned rights fall under the *auspices* of Article 8 ECHR. Indeed, the interpretation of the 'Right to respect for private and family life, home and

[119] Despite the impressively far-reaching impact the use of such a technology could have also with respect to other rights, for reasons of space this composition will mainly focus on the rights mentioned above because more relevant to the research perspective here adopted.

[120] Specific reference to this right is also made in Article 16(1) TFEU.

[121] See Article 1 and Recital (11) LED.

correspondence'[122] provided by the ECtHR encompasses several interests revolving around '*the principle of personal autonomy*'.[123] Hence including the right to personal development, to establish relationships with others, to self-determination and to '*informational self-determination, which implies control over one's own personal information*'.[124] In this respect, the Court's case-law focusing on the use of personal data '*in the law enforcement area*' is particularly abundant.[125] Moreover, the protection of personal data is also covered by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) recently amended in May 2018 through Protocol CETS No. 223.

For what concerns the right to freedom of assembly, it is recognised as a fundamental right under Article 12 CFR and Article 11 ECHR. Yet, as emerging by the well-established case-law of the ECtHR, it appears strictly connected also to the protection of the 'freedom of thought, conscience and religion' and to the 'freedom of expression'.[126] In fact, several times the Court took into account those rights in its assessment on whether or not a violation of Article 11 could be found.[127]

With regard to the relationship between the CFR and the ECHR, the latter together with the jurisprudence of the ECtHR are explicitly recalled in the preamble of the Charter. In turn, the preamble of the ECHR declares the commitment of the European countries to the collective enforcement of the rights proclaimed in the UDHR

[122] *e.g.* ECtHR, *Amann v. Switzerland,* 27798/95, 16 February 2000, para.65; *Rotaru v. Romania*, 28341/95, 4 May 2000, para. 43. At the universal level the right to privacy is recognised by Arts. 12 UDHR and 17 ICCPR.

[123] ECtHR, *Pretty v. the United Kingdom,* 2346/02, 29 July 2002, para.61; *E.B v. France*, 43546/02, 22 January 2008, para. 43, in this regard mentioned in De Vries K., *supra* note 12, 670.

[124] Kranenborg H., *Protection of personal data*, in *The EU Charter of Fundamental Rights: A Commentary*. Ed. Peers S., Hervey T., Kenner J. and Ward A., Hart Publishing, 2014, 223-265, 229; van der Sloot B., *Privacy as human flourishing: could a shift towards virtue ethics strengthen privacy protection in the age of Big Data*, J. Intell. Prop. Info. Tech. & Elec. Com. L., 5, 230-244, 234.

[125] *Ibid*, 228.

[126] Respectively enshrined in Arts. 9-10 ECHR and 10-11 CFR.

[127] In this sense Broeksteeg H., *Freedom of Assembly and Association*, in van Dijk P. *et al.*, *supra* note 12, 813-835, 815 *et seq.* and references therein.

of 1948.[128] More specifically, according to Article 6(3) TEU the rights guaranteed by the ECHR constitute general principles of EU law and wherever there is a correspondence between rights contained in the two instruments, the '*meaning and scope'* of the rights protected by the Charter *'shall be the same as those laid down by the said Convention*'.[129] Lastly, it is worth considering that whilst the protection of 'fundamental rights' contained in the Charter is ensured when the Member States '*are implementing Union law*',[130] the respect for the broader notion of human rights is one of the 'European founding values' whose respect, according to Article 2 TEU, is required independently from the application of EU law.[131]

Within this complex scenario, the two systems overlap while maintaining their different scopes and purposes of application. Yet, they interact and influence each other as demonstrated by the '*constant dialogue between the CJEU and the ECtHR, observed in numerous references*' in their jurisprudence.[132] However, this analysis will mainly refer to the ECtHR jurisprudence, since it gives many insights on the specific interactions between fundamental human rights and their limitations in the context of law enforcement activities.

From this perspective, in order to assess whether the use of FRT by law enforcement authorities is consistent with the European human rights law framework, it appears necessary to briefly reconstruct the conditions under which the rights object of this study can be lawfully limited.

---

[128] On the relevance of the universal human rights law for the CFR see Rosas A., *The Charter and Universal Human Rights Instruments,* in *The EU Charter*, *supra* note 133, 1685–1702. Therein on the relationship between the Charter and the Convention see Gragl P., *Agreement on the Accession of the European Union to the European Convention on Human Rights,* 1727-1824. See also Gerards J., *Relationship between the Convention and the EU*, in van Dijk P. *et al.*, *supra* note 12, 331-352.

[129] Article 52(3) CFR. More specifically on these themes Peers S. and Prechal S., *Scope and Interpretation of Rights and Principles*, in *The EU Charter of Fundamental Rights*, *supra* note 124, 1455–1522. See also *J.N. v Staatssecretaris van Veiligheid en Justitie*, case C-601/15 PPU, para. 77 where the CJEU specified the relevance of the rights as stated in the ECHR '*for the purpose of interpreting*' the analogous rights contained in the CFR.

[130] Article 51 CFR

[131] Rosas A., *supra* note 128, 1686-1687.

[132] EDPS, *Assessing the necessity of measures that limit the fundamental rights to the protection of personal data: A Toolkit*, 2017, 6 and the case-law therein mentioned in note 24.

2.2 The European Human Rights Law framework, the system of limitations.

The fundamental rights enshrined in the European human rights law system just described can be generally restricted in presence of the conditions set out in Article 52(1) CFR and according to the limitation clauses contained in the ECHR.[133] Although the wording of these provisions is not identical, any lawful interference with protected rights must: occur in presence of a legal basis, pursue a legitimate aim through proportionate measures, and be necessary in a democratic society.[134]

Each of these requirements is then cautiously applied by the Courts on a case-by-case basis to evaluate whether an identified interference with the rights involved is justified or not.[135] The assessment on the legitimacy of the aim pursued by a certain measure is the less problematic stage of such an evaluation. Indeed, aims like the protection of national security or the prevention and detection of crimes are generally deemed legitimate.[136] Consequently, the Courts' assessments focus more on the legality and proportionality tests.[137]

The presence of a legal basis to justify an interference with fundamental rights is not a just formal requirement. On the contrary, it entails different factors as the '*substantive*' respect for the domestic legal system and the '*quality of law*'.[138] The latter encompasses the accessibility of the law, a level of precision allowing the foreseeability

[133] Arts. 8-11 ECHR and Art. 15 'Derogation in time of emergency'.

[134] Cf. Arts. 8-11 ECHR and Art. 52(1) CFR. For instance, despite Article 52(1) CFR does not explicitly mention the 'democratic society' as a reference for the evaluation of the limitations it has been argued that '*the respect for democracy*' is one of the founding 'European values' enshrined in Art. 2 TEU and that Title II TEU (Arts. 9-12) contains already in its heading a clear reference to '*democratic principles*'; see Peers S. *et al.*, *supra* note 129, 1480.

[135] Lavrysen, L., *System of Restrictions*, in van Dijk P. *et al.*, *supra* note 12, 307-330, 308 *et seq.*

[136] *i.a.* ECtHR, *Leander v. Sweden,* 9248/81, 26 March 1987; *M.K. v. France*, 19522/09, 18 July 2013.

[137] Lavrysen, L., *supra* note 135, 314.

[138] Lavrysen, L., *supra* note 135, 311 *et seq.*

of its effects for an individual, and '*adequate safeguards'* against potential abuses by public authorities.[139] For instance, in *Huvig v. France*[140] the ECtHR specified the elements that must be provided by law in the context of criminal surveillance. These include: '*the categories of people liable to be monitored; the nature of the offences subject to surveillance; limits on the duration of such monitoring; the procedure to be followed for storing the data; the precautions to be taken when communicating the data; and the circumstances in which data is erased or destroyed*'.[141] Accordingly, the foreseeability required in the field of surveillance does not entail the consciousness of those being monitored but the availability of an '*adequate indication of the circumstances in which and the conditions on which*' such measures can occur.[142] As for the necessary safeguards, the ECtHR case-law encompasses the supervision (*e.g. Zakharov v. Russia*[143]) and the possibility of review (*e.g. Hasan and Chaush v. Bulgaria*[144]) of the measures interfering with the concerned rights by an independent authority.

Similarly, also the proportionality '*between rights and limitations*' requires a strict evaluation.[145] Indeed, in the context of the ECHR the requisite to strike a *'fair balance between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights*' has been declared as '*inherent in […] the Convention*'.[146] Hence, to be 'necessary in a democratic society' a measure should correspond to '*a pressing social need*'.[147]

Such an evaluation is particularly challenging for the Court, which has to take into account several factors, like '*the competing individual and community interests*

[139] *Ibid.*, 313.
[140] ECtHR, 11105/ 84, 24 April 1990.
[141] Malgieri *et al.*, *supra* note 113, 513.
[142] ECtHR, *Malone v. the United Kingdom*, 8691/79, 2 August 1984, paras. 67-68; see also *Weber and Saravia v Germany* (admissibility) 54934/00, 29 June 2006, paras. 93–95.
[143] ECtHR, 47143/06, 4 December 2015, para 302.
[144] ECtHR, 30985/96, 26 October 2000, para 85.
[145] Peers S., *et al.*, *supra* note 129, 1470 *et seq.*
[146] ECtHR, *N. v. the United Kingdom*, 26565/05, 27 May 2008, para. 44 as mentioned in Lavrysen L., *supra* note 135, 316.
[147] *Ibid.*

asserted by applicants and respondent States', the '*severity*' of the interference with a certain right, its context, the kind of right involved, and if that interference affects '*the core or the periphery of the right*' concerned.[148] For instance, in *Unuz v. Germany*, the Court recognised the monitoring of a person's movements through GPS surveillance as interfering with Article 8 ECHR. However, considering that such a measure was carried out for a *limited period of time* and in the *context* of an investigation for *serious crimes* related to terrorism, the Court did not find a violation of the applicant's rights.[149]

Once the essentials of the legal framework of this human-rights based study on law enforcement uses of FRT have been concisely outlined, what is left is its application to a set of paradigmatic examples.

3. The uses of Facial Recognition by law enforcement authorities.

3.1 Facial Recognition as a form of 'verification'.

Over the past few years, FRT steadily became an authentication tool for guaranteeing the access to and the use of personal devices just to their legitimate users.

In this way, their faces have been registered as an access key to "unlock" that specific device, consequently granting access to all the data therein stored. This increasingly widespread feature has generally been well-received by all those users who might consider this functionality as a playful breakthrough for the security of personal devices.

Authentication is the simplest of the three main functions FRT can typically perform. Indeed, "unlocking" a device with our face constitutes a *verification* task by which a device compares the user's face with a template image corresponding to the facial traits of the device's owner.[150]

---

[148] *Ibid.,* 319. On the last point Art. 52(1) CFR explicitly mentions the respect for '*the essence*' of rights and freedoms therein recognised.

[149] EctHR, 35623/05, 02 September 2010.

[150] Introna L., *supra* note 107, 187; Lynch J., *supra* note 112, 5.

This kind of *one-to-one* comparison is also utilised to an increasing extent in international airports where it optimises efficiency and waiting times at border controls. There, an FRS authenticates the travellers' identity verifying if the pictures in their passports match with the shot taken *in situ* by the automated machinery.[151]

At this point, the utilisation of FRT also in the exercise of States' full sovereignty at border checks invites us to reflect on the sensitiveness of the data extrapolated by AI in such situations. Indeed, once associated by competent authorities to other *personal data*,[152] passport pictures and fingerprints serve as *biometric templates* inextricably combining our personal details with our physiognomic traits.[153] Hence, *biometrics* or *biometric data* constitute a particularly sensitive and therefore protected category of personal data.[154] Examples of biometrics are '*iris scans, palm prints, voice prints, wrist veins, person's gait, and DNA*'.[155]

According to the relevant case-law, any processing of personal data, including their collection, storing, successive use or disclosure, constitutes itself an interference with the respective Articles 8 of both the CFR and the ECHR.[156] In this view, the EU system of data protection law or 'data privacy law' regulates those activities by

[151] FRA, *supra* note 17, 7.

[152] As our *attributed identifiers* (*e.g.* our name and surname) and *biographical identifiers* (*e.g.* our address, place, and date of birth). On the mentioned categories of '*identifiers*' see Introna L. *et al.*, *supra* note 112, 9. For the definition of personal data see Article 4(1) GDPR; Article 2, *Convention for the protection of individuals with regard to the processing of personal data*, ETS No. 108 (1981), today Convention 108+ as amended in May 2018 through Protocol CETS No. 223.

[153] *Privacy Impact Assessment Report*, *supra* note 115, 11.

[154] Biometric data '*means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*', see Art. 4(14) GDPR. Biometrics are considered among the '*Special categories of data*' under Convention 108+, the GDPR, and the LED. See respectively Art. 6, Art. 9, and Art. 10. On some of the most modern forms of biometrics, see Jiang R., Al-Maadeed S., Bouridane A., Crookes, D., & Beghdadi, A., *Biometric Security and Privacy*, Springer International Publishing, 2017. See also Introna I. *et al.*, *supra* note 111, 182; FRA, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, 2018.

[155] Lynch J., *supra* note 112, 4.

[156] *e.g.* CJEU, *Digital Rights Ireland*, joined cases C-293/12 and C-594/12, 8 April 2014, paras. 34-36; ECtHR, *S. and Marper v. the United Kingdom*, 30562/04 and 30566/04, 4 December 2008, para. 67.

providing a core of basic principles.[157] These include the lawful,[158] fair and transparent processing[159] of accurate and up to date data,[160] and the adequacy, relevance, and limited amount of that data, with respect to the aims of the processing (*i.e.* data minimisation principle).[161] Lastly, the purposes of the processing are due to be specified, explicit and legitimate since the collection of the information,[162] which – at least under the GDPR – should intervene upon the freely given consent of the data subject.[163]

With regard to the processing of biometrics, under Article 9(2) GDPR, it is generally prohibited and allowed just in a *numerus clausus* of cases therein mentioned. Then, according to Article 10 LED, the processing of such data should be allowed when '*strictly necessary'* and in presence of '*adequate safeguards for the rights and freedoms of the data subject*'.[164]

After these premises, it seems that – at least – the *verification* tasks pursued by FRSs while unlocking our smartphones or performing border controls identity checks do not lead to particular fundamental rights concerns. This of course as long as the consented purposes for the collection and processing of our biometrics are respected, and their confidentiality and security are guaranteed through the implementation of '*appropriate technical and organisational measures*'.[165]

---

[157] Bygrave, L. A., *Data privacy law: an international perspective*, Oxford University Press, 2014, mentioned in Caruana M., *supra* note 21, 250. For further details on the '*Key principles of European data protection law*', see European Union Agency for Fundamental Rights (FRA) and Council of Europe (CoE), *Handbook on European data protection law,* 2018 Edition, 2019.

[158] Cf. Art. 6 GDPR and Arts. 8, 9, 10 LED.

[159] Cf. Art. 5.1(a) GDPR and Art. 4.1(a) LED.

[160] Cf. Art. 5.1(d) GDPR and Art. 4.1(d) LED.

[161] Cf. Art. 5.1(c) and Art. 4.1(c) LED.

[162] Cf. Art. 5.1(b) and Art. 4.1(b) LED.

[163] Cf. Art. 7 GDPR and Recitals (36), (37) LED. Under Article 4(1) GDPR the data subject is '*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'.

[164] See also the other conditions required by Art. 10 LED.

[165] Art. 5(1)(f) GDPR; Art. 4(1)(f) LED. See also Art. 32(1) GDPR; Art. 29(1) LED.

Such provisions seem to follow the doctrine of *positive obligations* emerging from the ECtHR case-law with regard to Article 8. For instance, in *I. v. Finland*, the Court ruled on the inadequacy of the merely formal protection of special categories of data provided through not effectively enforced legislative measures.[166] A similar reasoning also emerged in *Craxi v. Italy* where the ECtHR specified that the protection afforded by Article 8 is not limited against '*arbitrary interferences by the public authorities*' but it involves '*positive obligations'* like the availability of '*appropriate safeguards […] to prevent any such disclosure of a private nature as may be inconsistent with the guarantees in Article 8*'.[167]

Yet, from a slightly different angle, even the most basic and less controversial uses of FRT may veil an alarming social reality. In our hyper-connected world, the more we become familiar with "freely give" our consent to perform the most disparate actions requiring the harvesting of our personal data, the more we steadily accept, endorse, and surrender to their exploitation.[168]

In the same logic, the more our images become connected with playful and apparently rewarding customer experiences or ephemeral profits, the more our perception of the strict connection between our appearance and our human nature is debased. When our lives growingly revolve around a frenetic spiral of images, videos, shots, camera-filters, etc., the users become more comfortable with the '*seemingly harmless applications of facial recognition tech*' growingly materialising around us.[169]

[166] ECtHR, 20511/03, 17 October 2008.

[167] ECtHR, 25337/94, 17 October 2003, paras. 73-74. See also OHCHR, *CCPR General Comment No. 16: Article 17-The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, Adopted at the 32nd Session of the Human Rights Committee, on 8 April 1988, para. 10.

[168] Cf. Zuboff S., *supra* note 10, 79.

[169] Stark L., *Facial recognition is the plutonium of AI*, XRDS: Crossroads, The ACM Magazine for Students, 25(3), 50-55, 55.

3.2 'I will tell who you are'. Facial Recognition performing identification tasks.

Whilst *verification* tasks consist of a *one-to-one* comparison, in the case of *identification*, 'still' or live-streamed images are used as a biometric sample and compared with a multitude of references. This kind of *one-to-many* search relies on pre-existent databases like those containing mugshots of offenders already convicted for certain crimes.[170]

In the field of law enforcement activities, such instruments are suitable for a variety of purposes. FRT can be used to easily verify if a (temporarily) unknown individual, caught by cameras while committing a crime, is instead a person already known to the authorities. This allows authorities to quickly pinpoint the suspect reconnecting the face captured in a video footage with the correspondent *attributed* and *biographical identifiers*, or to other data *e.g.* previous convictions.[171]

Conversely, facial recognition identifications can be used to detect if a person of interest – whose identity is known to the authorities – is within a monitored area, *e.g.* attending a sport event. This kind of identification is generally referred to as *watch list* verification.[172]

The potential benefits of such uses are evident. For instance, the International Criminal Police Organization (INTERPOL) runs different programmes based on biometrics, and particularly on facial recognition. Whilst the Project First (Facial, Imaging, Recognition, Searching and Tracking) is implemented for the identification of members of transnational terrorist groups or foreign terrorist fighters (FTFs),[173] the Face Recognition System (IFRS) is to date the biggest global criminal database. This database – thanks to the cooperation among more than 160 countries – made possible

[170] Davies B., *supra* note 114, 15.

[171] On the notions in italics see Introna L. *et al.*, *supra* note 112, 9. For an overview on different possible uses of face recognition by law enforcement see Garvie C., Bedoya A. M., Frankle J., *The Perpetual Line-Up – Unregulated Police Face Recognition in America*, Georgetown Law University, Center on Privacy & Technology, 2016, 10.

[172] Introna L. *et al.*, *supra* note 112, 13; FRA, *supra* note 17, 7-8.

[173] See the INTERPOL dedicated page available at https://www.interpol.int/Crimes/Terrorism/Identifying-terrorist-suspects.

since the end of 2016 the identification of '*more than 650 criminals, fugitives, persons of interest or missing persons*'.[174] Considering these great capacities, the widespread use of such tools in the US[175] and their recent upsurge also in the EU will not surprise.[176]

According to well-established jurisprudence of the European Commission of Human Rights, the storage and subsequent use of pictures taken by law enforcement agencies consequently to an arrest does not constitute itself an interference with Article 8 ECHR.[177] Yet, the operating modes of advanced facial recognition software today available on the market appear incredibly problematic.

This is the case of a newly developed facial recognition research tool designed to help '*law enforcement agencies to identify perpetrators and victims of crimes*'.[178] In

[174] See the INTERPOL dedicated page available at https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition.

[175] In a hearing conducted by in 2017 to review the law enforcement use of FRT it emerged that 18 states have *memoranda* of understanding with the FBI to share with them databases. As a result, more than half of American adults are in those databases without even knowing it. See The US House Committee on Oversight and Reform, Hearing '*Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*', 2154 Rayburn House Office Building, Washington, DC, 22 May 2019, available at https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and.

[176] According to EDRi – European Digital rights '*As of May 2020, at least 15 European countries have experimented with biometric technologies such as facial recognition in public spaces, for purposes which lead to mass surveillance*', the number is referred to '*Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, the Netherlands, Poland, Romania, Serbia, Slovenia, Sweden, Switzerland and the UK*', see Jakubowska E. *et al.*, *supra* note 93, 7. See also Kayser-Bril N., *At least 10 police forces use face recognition in the EU*, Algorithm Watch, published on 11 Dec. 2019, available at https://algorithmwatch.org/en/story/face-recognition-police-europe/; Campbell Z. & Jones C., *Leaked reports show EU police are planning a pan-European network of facial recognition databases*, The Intercept_, published on 21 Feb. 2020, available at https://theintercept.com/2020/02/21/eu-facial-recognition-database/.

[177] *X v. the United Kingdom*, 5877/72, Commission decision of 12 October 1973, Decisions and Reports (DR) 45, 94; *Lupker v. the Netherlands*, no. 18395/92, Commission decision of 7 December 1992, unreported, *Kinnunen v. Finland*, no. 24950/94, Commission decision of 15 May 1996, unreported; and *Friedl v. Austria*, no. 15225/89, Commission decision of 16 May 1996, unreported, as mentioned in ECtHR, *Gaughran v. United Kingdom*, , 45245/15, 13 June 2020, para. 65.

[178] See the company website https://clearview.ai/.

fact, since early 2020, the US-based firm *Clearview AI* raised diffuse concerns despite its declared commitment towards increased levels of public safety.[179]

During an interview on CNN Business conducted in February 2020,[180] the founder of Clearview described this tool as '*a search engine for faces*'. Once a facial image is uploaded on the system,[181] it conducts a reverse image search against a database much wider than the one utilised by the FBI.[182]

If on the one hand, the unprecedented vastness of this dataset is one of the greatest features of this product, one the other hand, one might wonder how this start-up can have gathered such an extensive amount of facial images. As declared in the mentioned interview, this tool uses a *scraping algorithm* that collects and stores every picture accessible on the internet from '*millions and millions of different websites*'. These include Google and YouTube, and social networks as Facebook, Twitter and LinkedIn. Some of these 'tech-giants' have already sent cease-and-desist letters to Clearview AI labelling its methods as inconsistent with their 'Terms and Conditions' policies.[183] In turn, the company stresses that those images are openly accessible on the

[179] Hill K. *The Secretive Company That Might End Privacy as We Know It*, The New York Times, 18 Jan. 2020, available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[180] O'Sullivan D., *This man says he's stockpiling billions of our photos*, CNN Business, 10 Feb. 2020, available at https://edition.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html. For the extended version of the interview available on the YouTube channel of CNN Business follow the link https://youtu.be/q-1bR3P9RAw.

[181] In the EFF report, *supra* note 121, it is underlined how these uses allow to '*search and identify people in photos of crowds and in pictures posted on social media sites – even if the people in those photos haven't been arrested for or suspected of a crime*', 20, see also Article 6 LED.

[182] Whilst the tech-firm's database allegedly includes '*billions and billions*' of pictures, in 2017 the FBI thanks to the cooperation of about 18 American States, could access to mugshots and pictures of approximately half of the American adults. Cf. The US House Committee on Oversight and Reform, Hearing, '*Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*', *supra* note 175 and the beforementioned CNN interview.

[183] *Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement***,** CBS NEWS, 5 Feb. 2020, available at https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/; Bonifacic I., *Google tells facial recognition startup Clearview AI to stop scraping photos*, engadget, 5 Feb. 2020, available at https://www.engadget.com/2020-02-05-google-tells-clearview-at-stop-scraping-photos.html.

internet and therefore freely collectable. Clearview AI declared that it will continue to work as it has done so far, and that it is ready to face possible litigations in court since its policy '*is in compliance with all the different privacy laws from around the world*'.[184] In this regard, Clearview AI – already in use by approximately 600 North American law enforcement agencies[185] – has offered trial versions of its tool to '*at least 26 countries outside the US'* including *'Australia, Belgium, Brazil, Canada, Denmark, Finland, France, Ireland, India, Italy, Latvia, Lithuania, Malta, the Netherlands, Norway, Portugal, Serbia, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom*'.[186] Yet, the indiscriminate collection, retention and commercial use of European citizens' personal data seems against the most basic EU data protection law principles.

For instance, Article 5.1(b) GDPR requires that personal data must be '*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*'.[187] From this perspective, the exploitation of the consent to 'Terms and Conditions' of *e.g.* a social network, given by users publishing their pictures might be intended as a *function creep*. Namely, *'the expansion of a process or system, where data collected for one specific purpose are subsequently*

[184] See the CNN interview.

[185] See the CNN interview.

[186] Amongst the recipients also the INTERPOL, which benefited from a 30-day trial version as the General Secretariat in Lyon confirmed, see Mac R., Haskins C. and McDonald L., *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BuzzFeed News, 27 Feb. 2020, available at https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement. Another BuzzFeed News shows a map allegedly part of a presentation aimed at attracting clients through the 'rapid international expansion' of the company. Among the countries involved – as partners or potential partners – pop up also Nigeria, Qatar, Singapore *et al.* certainly well-known for their human rights abuses. See Haskins C., Mac R., McDonald L., *Clearview AI Wants To Sell Its Facial Recognition Software to Authoritarian Regimes Around The World*, 5 Feb. 2020, available at https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22.

[187] Article 5.1(b) GDPR.

used for another unintended or unauthorized purpose'.[188] Indeed, for the 'Lawfulness of [the] processing', Article 6.1(a) GDPR requires the consent of the data subject for the *specific purposes of each processing* of personal data.[189] Particularly, Article 9 GDPR prohibits the processing of certain categories of data – including *biometrics*.[190]

For the processing of these special categories of data, Article 9.2(a) requires the '*given explicit consent […] for one or more specifies purposes'*. An exception to this rule is provided by let. (e), where the consent is no more required for that '*personal data which are manifestly made public by the data subject*'.

Probably to invoke this exclusion, the founder of Clearview AI repeatedly specified that all the information stored for the functioning of the software are publicly available. Yet, under European data protection law this is not the case. According to Recital(51) GDPR, the mere processing of photographs, like those uploaded on social media, does not *per se* entail the processing of the *biometrics* FRT can extract from those pictures. In other words, just once those pictures are processed '*through a specific technical means allowing the unique identification or authentication of a natural person*' – as in the case of Clearview AI – the data contained in the picture qualify as biometrics. Consequently, neither the mere availability of a picture of oneself on the internet nor its voluntary upload on social media can amount to making manifestly available biometric data in the meaning required by the GDPR for their processing.

Furthermore, additional concerns are given by the impressive capabilities showed by this specific application of FRT in some demonstrative tests.[191] In one of those, the software was able to retrieve instantaneously dozens of photos from the most diverse sources, including an image representing the "wanted individual" posing for a group picture taken '*more than a decade before*'.[192] Indeed, by focussing on the most salient facial features, this tool is capable of successfully detecting a target among a

[188] Mordini E., *Ethics and Policy of Biometrics*, in Tistarelli M., Li S. Z. and Chellappa R. (Eds), *Handbook of Remote Biometrics for Surveillance and Security*, Springer, 2009, 293-312, 294.

[189] Article 6.1(a) GDPR

[190] Article 9 GDPR

[191] See the CNN interview

[192] *Ibid.*

crowd and despite the ageing. Impressive results were also achieved in simulated adverse conditions, *i.e.* the partial obstruction of the target's face.[193] During another test, the search results included pictures from an Instagram *private* account theoretically accessible just to 'authorised circles' of followers.

If the massive and unauthorised scraping of personal data was not enough, this episode could be the sign that this algorithm is able to unlawfully bypass the privacy restrictions adopted by final users. However, the firm's CEO claims such outcomes are resulting from a 'scraping' occurred in the past, when the account was probably 'openly accessible'.[194] If so, the episode shows that the algorithm not only stores personal data without any legal basis, but it does not even take into account the successive deletion of stored items or changes in the privacy settings operated by the legitimate user of *e.g.* a social network. Once again, this is against the basic data protection principle which puts the data subject 'in control' of its personal data.

These events raised significant concerns among European citizens whose 'faces' could already have been collected and stored without any consent, and the European Commission is monitoring the 'situation'[195] whilst in contact '*with national data protection authorities and the European Data Protection Board*'. [196] The latter

[193] *Ibid.*

[194] *Ibid.*

[195] Similarly, also the Australian Privacy Commissioner Angelene Falk. See Tighe A., *The Australian behind Clearview AI, a facial recognition software, says it is being used here*, The World Today ABC, 17 Mar. 2020, available at https://www.abc.net.au/news/2020-01-23/australian-founder-of-clearview-facial-recognition-interview/11887112; Sadler D., *OAIC investigates 'dangerous' face recognition app*, Innovation Aus, 28 Jan. 2020, available at https://www.innovationaus.com/oaic-investigates-dangerous-face-recognition-app/. Of the same opinion also the US Senator Ron Wyden who through a 'tweet' labelled the company's product as '*extremely troubling*', see *Clearview AI: Face-collecting company database hacked*, BBC NEWS, 27 Feb. 2020, available at https://www.bbc.com/news/technology51658111?intlink_from_url=https://www.bbc.com/news/topics/c12jd8v541gt/facial-recognition&link_location=live-reporting-story.

[196] Stolton S., *After Clearview AI scandal, Commission 'in close contact' with EU data authorities*, EURACTIV, 12 Feb. 2020, available at https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/.

recently expressed serious doubts about the legitimacy of Clearview AI use by EU law enforcement authorities and its consistency with the EU data protection framework.[197]

Moreover, also the defiant attitude towards public concerns and cease-and-desist letters of this company sounds alarming. It recalls the schemes of '*infrastructure imperialism*' in the past operated even by other data ventures which enacted '*incursions into legally and socially undefended territory until resistance is encountered*'.[198] In this respect, Zoé Vilain – Privacy Chief & Strategy Officer of the French start-up Jumbo – has just filed an official complaint before the French Data Protection Authority (CNIL).

In fact, Clearview AI – after an initial reluctance in itself contrary to GDPR provisions[199] – confirmed that its database contains Vilain's pictures.[200] If such facts were further confirmed, Clearview could be sanctioned by the CNIL with an administrative fine of €20.000.000 or up to the '*up to 4 % of the total worldwide annual turnover*'.[201]

To conclude, whenever during the mentioned CNN interview, the Clearview CEO had to confront uncomfortable topics related to privacy, consent, or the potential misuse of his tool, he used a common "catch-all argument" which is worth reflecting on. That is, "the good cause" his product is used for. Yet, such narratives based on "the pursuit of a higher level of security" result not convincing when challenged with the aforementioned mass-scale and systematic violations of the right to data protection.

Moreover, a few years ago, the same reasoning was promoted by the chief executive of the company LLVision. Trying to debunk public concerns about AI-based facial recognition smart-glasses, he declared that people '*should not be worried about privacy concerns because […] authorities were using the [company's] equipment for*

[197] EDPB, *Response to MEPs concerning the facial recognition app developed by Clearview AI*, 10 Jun. 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf.

[198] On this concept see Zuboff S., *supra* note 10, 78, 79, and the literature therein mentioned.

[199] Recital(59) and Arts. 13 *et seq.* GDPR

[200] Jumbo Privacy Blog, *Jumbo Privacy brings a formal GDPR complaint against Clearview*, 14 Jul. 2020, available at https://blog.jumboprivacy.com/jumbo-privacy-brings-a-formal-complaint-against-clearview.html.

[201] Art. 83 GDPR, see also Arts. 58, 60, and 84.

"noble causes", catching suspects and fugitives from the law'. If we consider that the 'authority' he referred to is the Chinese Government,[202] and that, such smart-glasses were used to detect people from a 'blacklist-database', such arguments are definitely not heartening.[203] In this regard, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye reported that:

> *[p]erhaps no other environment demonstrates the comprehensive intrusiveness of these technologies better than China. Credible reporting suggests that the Government of China, using a combination of facial recognition technology and surveillance cameras throughout the country, "looks exclusively for Uighurs based on their appearance and keeps records of their comings and goings for search and review".*[204]

Particularly the severe repression of Muslim minorities in northwest China, where an estimated million of people is held in "re-education camps" and deprived of any fundamental rights shows how modern technology can be easily used against targeted groups as an instrument for oppression.[205] Like a movie already seen the labelling of minorities as "violent extremist groups" becomes the rationale for terrible human rights violations.[206]

---

[202] In its 2020 country report, Freedom House labels China as 'Not Free' for the extremely low level of political and civil rights ensured to its citizens, see the report at https://freedomhouse.org/country/china/freedom-world/2020. The WJP Rule of Law Index 2020 ranked China 88th out of 128 countries considered, see the report available at https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index-2020..

[203] Li P. & Cadell C., *China eyes 'black tech' to boost security as parliament meets*, Reuters, published on 10 Mar. 2018, available at https://www.reuters.com/article/us-china-parliament-surveillance/china-eyes-black-tech-to-boost-security-as-parliament-meets; about the use of the same technology in Zhengzhou, see *Chinese police spot suspects with surveillance sunglasses*, BBC NEWS, published on 7 Feb. 2018, available at https://www.bbc.com/news/world-asia-china-42973456.

[204] Kaye D., *Surveillance and Human Rights*, UN Doc. A/HRC/41/35, 2019, para. 12.

[205] Wang M., *The Robots are Watching Us*, Human Rights Watch, 6 Apr. 2020, available at https://www.hrw.org/news/2020/04/06/robots-are-watching-us.

[206] *Ibid.*

4. Facial Recognition and categorisation. Towards emotional surveillance?

The section just concluded showed how FRT's functionalities are not limited to the detection of faces within a database of 'static' images. For instance, the targeting of certain ethnic groups based on specific facial characteristics is possible thanks to algorithmic *categorisation*.[207] Indeed, FRSs can categorise facial traits on different grounds like age, sex, colour of the skin, shape of the face or facial expression.[208] This last category has recently raised significant concerns since it would be used to identify people's emotions.[209] Yet, the inference of inner feelings by the scrutiny of facial expressions is nothing new.

In this regard, thanks to the work of Paul Ekman, 'the classical theory of emotions' became popular in psychological research since the second half of the twentieth century.[210] In the past, his theses have been used to train 'behaviour detection officers', and today are applied by AI[211] in the rapidly growing area of 'Affect Recognition'[212] or 'Emotion Recognition'.[213]

In this field, recent research claims that the detection of anger, disgust, fear, happiness, sadness, and surprise[214] does not even require the movement of facial muscles – *i.e.* an actual expression. In such cases, FRT analyses the facial colour due

[207] FRA, *supra* note 17, 8.

[208] *Ibid.*

[209] Schwartz O., *Don't look now: why you should be worried about machines reading your emotions*, THE GUARDIAN, 6 Mar. 2019, available at https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science; FRA, *supra* note 17, 8.

[210] *e.g.* Ekman P., Sorenson E. R. & Friesen W. V., *Pan-cultural elements in facial displays of emotion*, Science, 164(3875), 1969, 86-88; Ekman P., *Universal Facial Expressions of Emotion*, California Mental Health Research Digest, 8(4), 1970, 151-158. Or visit the webpage https://www.paulekman.com/.

[211] Schwartz O., *supra* note 209.

[212] AI Now, *Report 2019*, 50.

[213] THALES, *supra* note 112. The way of functioning of such instruments is further explained using as example Microsoft 'MS Face' software in Crampton J. W., *Platform biometrics*, Surveillance & Society, 17(1/2), 2019, 54-62.

[214] These the basic emotions according to Ekman P. & Friesen W. V., *Unmasking the face: A guide to recognizing emotions from facial clues*, Prentice-Hall, 1975; see also AI Now, *Report 2018*, 14.

to '*changes in blood flow or blood composition triggered by the central nervous system*'.[215] Other interesting cases recently observed involve a highly debated academic paper asserting that AI '*is more accurate than humans at detecting sexual orientation from facial images*'.[216] One of its authors also declared that '*sexual orientation was just one of many characteristics that algorithms would be able to predict through facial recognition*'.[217] In this sense, academic studies argued the possibility to make '*Automated Inference on Criminality using Face Images*'.[218] What is more, FRSs making predictions on one's personality or criminal predisposition to identify terrorists or paedophiles are already commercially available.[219] Also, a top purveyor of '*FBI, Interpol, London Metropolitan Police, and Honk Kong Customs'* declared to have included *'emotion detection, to its [facial recognition] software'.*[220]

Such technologies, allowing to detect potential terrorists among crowds through "unusual" or "concerning" expressions, attitudes, or behaviours, sound very promising. Yet, the theory these techniques are based on has recently been refuted. A number of scholars and experts claim that '*there are no universal emotions located in the brain […]. Rather, each experience of emotion is constructed out of more basic parts'*.[221]

---

[215] The quote is from the article *'At first blush, you look happy-or sad, or angry'* 19 Mar. 2018 on Ohio State News, available at https://news.osu.edu/at-first-blush-you-look-happy--or-sad-or-angry/. For this study see Benitez-Quiroz C. F., Srinivasan R. & Martinez, A. M., *Facial color is an efficient mechanism to visually transmit emotion*, Proceedings of the National Academy of Sciences, 115(14), 3581-358, 2018. For a video explanation of it follow the link https://youtu.be/xFmHU5yC3-A for the presentation '*Facial Color Transmits Emotion'*.

[216] Wang Y. & Kosinski M., *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*, Journal of personality and social psychology, 114(2), 2018, 246.

[217] Levin S., *Face-reading AI will be able to detect your politics and IQ, professor says*, The Guardian, 12 Sep. 2017, available at https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski.

[218] Wu X. & Zhang X., *Automated Inference on Criminality using Face Images*, *arXiv preprint arXiv:1611.04135*, 2016, 4038-4052.

[219] Schwartz O., *supra* note 209. See also the webpage of the Israeli company 'Faception – Facial Personality Analytics', https://www.faception.com/our-technology

[220] See AI Now, *Report 2019*, 50.

[221] Schwartz O., *supra* note 209, referring to Barrett L. F., *How emotions are made: The secret life of the brain*. Houghton Mifflin Harcourt, 2017.

Accordingly, individual emotions are a composite reality resulting from a variety of elements, such as environmental or cultural factors, interpersonal interactions *etc*.[222] The range of possible combinations is so diverse that '*[w]hile one person might scowl when they're angry, another might smile politely while plotting their enemy's downfall*'.[223]

From a slightly different angle, empirical evidence from a recent paper warn about the individual and societal risks arising from the deployment 'emotion recognition'. During this study, participants described emotions as '*intimate, personal, vulnerable, complex and hard to define*'.[224] According to them, 'emotional data' could be exploited for '*political or social control*' hence '*providing greater and greater potential for a fascist or totalitarian regime*'.[225]

Particularly in the field of crime control and prevention, the application of algorithms to infer – with affirmed scientific certainty – individual's innermost characteristics as emotions, personality, sexual orientation or if one is telling the truth or is lying,[226] should not be accepted. For instance, Article 11(1) LED prohibits any '*automated processing […] which produces an adverse legal effect concerning the data subject*' whenever such processing does not occur in force of a legal basis containing adequate safeguards for the rights and freedoms of those involved. Among these safeguards, explicit mention is made to '*the right to obtain human intervention on the part of the controller*'.[227] Yet, which level of guarantees a human intervention could

[222] *Ibid.* A similar view is also expressed by Barrett L. F., Adolphs R., Marsella S., Martinez A. M., & Pollak S. D., *Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements*, Psychological Science in the Public Interest, 20, 1–68, according to which '*facial configurations […] are not "fingerprints" or diagnostic displays that reliably and specifically signal particular emotional states regardless of context, person, and culture*'. See also AI Now, *Report 2018*, 14-15; AI Now, *Report 2019*, 51.

[223] *Ibid.*

[224] See Andalibi N. & Buss J., *The Human in Emotion Recognition on Social Media: Attitudes, Outcomes, Risks*, In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, 1-16.

[225] *Ibid.*

[226] FRA, *Facial recognition*, *supra* note 106, 8; Crampton J. W., *supra* note 212, 54, for the use of '*Automated Deception Detection System[s]* (*ADDS)*' to strengthen border controls. On the theme of emotion analysis see also Schwartz O., *supra* note 211.

[227] Article 11 LED.

offer with regard to inferences about human inner states made by facial recognition software appears doubtful. Indeed, while technologies perform increasingly sophisticated tasks, the single steps contributing to the outcome of their operations become impenetrable even to the most proficient of the experts. This phenomenon referable to any '*AI system whose innerworkings and rationale are opaque or inaccessible to human understanding*' is known as '*black box effect*'.[228] In this way, statistical results offered by impenetrable automated processes would mask under '*the glow of hard scientific fact[s]*'[229] suspicion and speculative predictions based on constellations of small fragments of data.[230] Particularly when the scientific literature on the theme is characterised by significant inconsistencies,[231] instead of being the ground for law enforcement activities, opaque and inexplicable algorithmic-systems should generate human uneasiness and untrustworthiness.[232]

Then, from a broader perspective, the rapid development of similar technologies may result in dangerous backsliding towards new forms of physiognomic criminology. For instance, Cesare Lombroso – father of the Italian School of Positivist Criminology – used data analysis to build models labelling homeless, vulnerable, and marginalised categories of people as more prone to crime.[233]

In light of this, the view of a criminal justice system designed to punish individuals for "what they are or think" instead of "what they do" appears a slippery

---

[228] Information Commissioner's Office & The Alan Turing Institute, *Explaining decisions made with AI, Part: 2*, 2019, 38.

[229] Wilson D. *et al*., *supra* note 95; Manheim K. *et al*., *supra* note 33, 109. On the '*the "veneer of objectivity" around high-tech systems*', Raso F. A. *et al*., *supra* note 1, 22.

[230] According to Raso F. A. *et al*., *supra* note 22, '*AI techniques can be used to discover some of our most intimate secrets by drawing profound correlations out of seemingly innocuous bits of data*'.

[231] On the existence of '*competing theories of emotion*' also Crampton J. W., *supra* note 212, 59.

[232] Miller K., *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, Journal of Technology Law & Policy 19(1), 2014, 105-146, 136; Manheim K. *et al*., *supra* note 33, 111, where '*AI results are often based on reasoning and processing that are unknown and unknowable to humans*'. Trustworthiness is mentioned as an essential factor for the evaluation of procedural justice in criminal matters in Simmons R., *Big data and procedural justice: Legitimizing algorithms in the criminal justice system*, Ohio State Journal of Criminal Law, 15(2), 2018, 573-582.

[233] *e.g.* Lombroso, C., L'uomo delinquente (1876). *Hoepli*, 1971.

slope and the use of not completely reliable, tested, and scientifically proved technologies to scrutinise the innermost corner of the complex human nature is spine chilling.[234] In one of the above-mentioned studies, the participants associated the use of emotion recognition with thoughts encompassing: '*control, manipulation, exploitation; unfair harm distribution; negative mental health impacts; identity misrepresentation including beyond one's lifetime; and challenges with holding algorithms responsible*'.[235]

Whilst emotions are hard to interpret even for those directly experiencing them the crave for grasping inner states and especially their assessment by private companies seems unreasonable.[236] In fact, a misinterpretation of intangible states would have tangible consequences particularly in areas 'prone' to abuses. We have already seen how significant the power of concepts as "security" is for the acceptance of intrusive measures among highly intimidated societies. From this standpoint, it is not hard to imagine how individuals and communities could be easily governed and manipulated using their emotions.

5. Reality mining and the use of live Facial Recognition.

The critical issues connected to FRT are not limited to the uses shown by the cases just analysed. Indeed, FRSs have a disruptive potential also when combined with the pervasive CCTV systems populating our cities.[237] This form of real-time facial video surveillance[238] involves the perpetual facial recognition processing of the images

[234] Similarly, AI Now, *Report 2019*, 51.
[235] Andalibi N. *et al*., *supra* note 229, 551.
[236] Similar concerns are shared also by Kaye D., *supra* note 204.
[237] Introna *et al.*, *supra* note 111, 184; see also Introna L. *et al.*, *supra* note 112, 20.
[238] Or "*'live facial recognition technology'* as a '*specific form of video surveillance*', see FRA, *Facial recognition technology*, *supra* note 106, 3. See also Fussey P., & Murray D., *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*, The Human Rights, Big Data and Technology Project, University of Essex, 2019, 19.

captured by CCTV systems within their range of action.[239] These uses obviously take place in public areas, here intended as

> *place[s] which can be in principle accessed by anyone freely, indiscriminately, at any time and under any circumstances. Public areas are open to the public. In principle anyone at anytime can have the benefit of this area. A person benefits freely from public areas. Public areas are governed by public authorities whose power to enforce the law and intervene are wider than within private property.*[240]

In such circumstances, if the machine identifies a match with a face previously set as a target it will trigger an alarm[241] – '*colloquially referred to as a "hit"*'.[242]

Even though the possibility to identify and locate persons of interest through FRSs is the most immediate use one might think of, another application of these systems also allows to trace missing persons, in particular children.[243] For instance, in India – one of the countries with the highest number of missing children in the world – after only four days of deployment by the police of New Delhi, approximately 3000 children have been identified and reconciled with their families.[244] In the same manner,

---

[239] Cf. Davies B. *et al.*, *supra* note 114, 9.

[240] '*Examples of relevant public areas […] include: public parks, pedestrian streets in the city centers, outdoor public parking areas, residential neighborhood streets, areas such as sports arenas and subway stations. Some public areas like universities, discos or cafés, that may be considered as semi-public areas*', see Commission for democracy through law (Venice Commission), *Opinion on video surveillance in public places by public authorities and the protection of human rights* [CDL-AD(2007)014], 2007, 4. See also the definition provided by UNESCO, *Inclusion Through Access to Public Space*, 2017, available at http://www.unesco.org/new/en/social-and-human-sciences/themes/urban-development/migrants-inclusion-in-cities/good-practices/inclusion-through-access-to-public-space/.

[241] Davies B. *et al.*, *supra* note 114, 9. See also Fussey P. *et al.*, *supra* note 238.

[242] Davies B. *et al.*, *supra* note 114, 13.

[243] Introna L. *et al.*, *supra* note 112, 20.

[244] Cuthbertson A., *Indian police trace 3,000 missing children in just four days using facial recognition technology*, Independent, 24 Apr. 2019, available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html.

this technology could be used to detect '*disoriented missing adults*' suffering from neurodegenerative diseases such as dementia or Alzheimer's disease.[245]

Yet, when *live facial recognition* is used for surveillance or security purposes there is a *caveat* for those who would instinctively associate its risks to those of common CCTV systems. In this sense, the processing of simple video surveillance images capturing the '*physical, physiological or behavioural characteristics of a natural person*' does not require the application of the enhanced levels of data protection prescribed for *biometrics*. However, the respect of those higher standards becomes necessary whenever that data is processed '*for the purpose of uniquely identifying a natural person*'.[246] This is the case of the enhanced levels of intrusiveness reached by the 'real-time *biometric processing* of video imagery' of live FRT.[247]

Moreover, the deployment of these *silent technologies* is characterised by a high degree of secretiveness, a passive role and a scarce involvement of the 'user/target', whilst – as seen earlier in this chapter – their inner functioning is opaque and inscrutable as a '*black-box'*.[248]

In the EU, this form of 'algorithmic surveillance'[249] has mostly been deployed in controlled circumstance or for 'testing purposes'.[250] Yet, these experiments denote a concerning interest of public authorities towards more systemic implementations of these insidious technologies. As it will be shortly clearer, what live FRT puts at risk goes way further than the respect for the right to data protection.

---

[245] Or for people suffering from amnesia, having an epileptic seizure or a psychotic episode, see THALES, *supra* note 112; see also Girasa R., *supra* note 23, 116 and note 43.

[246] EDPB, *supra* note 108, 15.

[247] Fussey P. *et al*., *supra* note 238, 19 and there note 18.

[248] On the distinction between 'silent' and 'salient' technology see Introna L. *et al*., *supra* note 112, 183. The algorithms on which this technology is based are referred to as '*black boxed*' in Davies B., *et al*., *supra* note 114, 12, 40, 43.

[249] Introna L. *et al*. *supra* note 109.

[250] See *inter alia* the examples mentioned in FRA, *supra* note 17, 3. Or the detailed reports about the trials conducted by the London Metropolitan Police Service and the South Wales Police; respectively Fussey P., *et al*., *supra* note 238, and Davies B., *et al*., *supra* note 114.

5.1 From test to test: between data protection law infringements and side effects.

This and the following section will be primarily based on two academic reports by (1) the Cardiff University and (2) the University of Essex. These documents provide insights on some live FRT test deployments conducted, between 2017 and 2018, by UK law enforcement authorities.[251] Such reports, allow to draw the attention on several issues emerging from the episodes therein described, however, those events will be here further analysed using the perspective distinctive of this paper.

The use of live FRT for the detection of persons of interest, suspects, fugitives, or troublemakers, usually operates against a pre-set database of targets named '*watch list*'.[252] In one of our examples, this included various sub-lists, each labelled with a colour corresponding to the level of 'threat' represented by those therein enlisted.[253] However, both the reports at issue repeatedly pointed out the lack of any '*specific rationale*' for the construction of the different lists.[254]

On this point, using as a reference Article 6 LED, the design of such *watch lists* should be regulated accurately, distinguishing the different categories of people involved. In particular, Article 6 requires the distinction among '*suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses; persons possessing relevant information or contacts; and associates of suspects and convicted criminals'*.[255] Recital (31) LED frame this requirement within the respect for '*the right of presumption of innocence as guaranteed by the Charter [of fundamental rights] and by the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively*'.[256]

---

[251] See respectively, Davies B., *et al*., *supra* note 114 and Fussey P., *et al*., *supra* note 238.
[252] *Ibid*. See also FRA, *supra* note 17, 3; Introna L., *supra* note 121, 13.
[253] Davies B., *et al*., *supra* note 114,12.
[254] Cf. *Ibid.*,12, 16, 40; Fussey P., *et al*., *supra* note 238, 11-12.
[255] Recital (31) and Article (6) LED. For some reflections about the conceptual difficulties of such a categorisation see Leiser, M. R., & Custers, B. H. M., *The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680*, European Data Protection Law Review, 5, 12, 2019, 11.
[256] Recital (31) LED.

Indeed, similar requirements clearly follow the leads of *S. and Marper v. the United Kingdom*. In this landmark case, the ECtHR considered the retention of biometric data for crime prevention and detection as pursuing a legitimate aim. Yet, particularly, the '*risk of stigmatisation*' and the frictions with the presumption of innocence deriving from the contested measure made it result 'not necessary in a democratic society'. Consequently, the Court labelled the indiscriminate retention of biometrics pertaining to different categories of persons as '*a disproportionate interference with […] the right to respect for private life*'.[257]

These principles have been recently recalled in *Gaughran v. the United Kingdom*. On this occasion, the Court found the indefinite retention of a 'custody photograph' violating Article 8 because '*[at present] the police may also apply facial recognition and facial mapping techniques to the photograph*'. In fact, this key component made insufficient the argument put forward by the responding State, which claimed the retention of pictures in a '*standalone database*' with limited access 'not in violation of Article 8'.[258] It is interesting to note how in this decision the ECtHR stressed the necessity to assess contemporary privacy violations with special scrutiny of technological advancements. In the Court's view, such instruments create risks of arbitrariness, rendering the exercise of state powers '*obscure*'.[259]

If we consider that also mere technical failures, due to the error-rate of the instruments deployed, may significantly impact on individual and community lives, similar perceptions might result even more founded.

During the tests conducted in South Wales, several people have been arrested thanks to the deployment of FRT. Yet, also a high number of *false positives matches* has been recorded.[260] Once acknowledged the match as 'false', the officers invited the people improperly stopped to verify with their eyes the erroneous match proposed by the system. This practice, aiming at 'justifying' the incidents occurred, can be claimed

[257] ECtHR , *S. and Marper v. United Kingdom*, 30562/04 and 30566/04, 4 December 2008, paras. 125; 122.
[258] *supra* note 177, paras. 67; 70.
[259] *Ibid.* para. 86.
[260] *Ibid.*, see the figures, 21-29. See also Fussey P., *et al.*, *supra* note 238, 116.

to be itself a further violation of the protection of personal data, as it implies the arbitrary, unlawful and unnecessary disclosure to third parties of the biometrics contained in the *watch list*. Under the GDPR, the disclosure of 'video footage to third parties' is to be considered a '*separate kind of processing*', possible just in presence of the legal bases listed in Article 6.[261] Moreover, Articles 14, 24 and 25 LED provide a number of safeguards to protect against arbitrary disclosure of personal data to third parties. These include *i.a.* (1) the right of the data subject to obtain information about the '*recipients to whom the personal data have been disclosed*';[262] (2) the obligation to maintain a record of the processing activities including '*the categories of recipients to whom the personal data have been or will be disclosed*',[263] and (3) the obligation to maintain '*logs of consultation and disclosure [that] shall make it possible to establish the justification, date and time*' of processing to be maintained '*for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data*'.[264]

Once again referring to *S. and Marper*, '*detailed rules*' about '*access of third parties [and] procedures for preserving the integrity and confidentiality of data*' are listed among the necessary guarantees required to avoid risks of '*arbitrariness*'.[265]

Whilst the officers appeared frustrated by the high rate of false positives, the people involved have 'positively' reacted to these accidents.[266] Nevertheless, displeasing episodes have also been recorded. Among these, the case of a young woman upset because her face had been coupled with the one of a middle-aged "wanted woman" present in the watchlist or a man who showed signs of anxiety given by the possibility to be erroneously stopped again in the future.[267]

---

[261] EDPB, *supra* note 108, 12-13; Article 6, for the definition of 'disclosure' and 'third parties' under the GDPR see also Article 4(2),(10).

[262] Article 14(c) LED.

[263] Article 24(1)(c) LED.

[264] Article 25(1),(2) LED. For the disclosure of 'video footage to third parties' under the GDPR see EDPB, *supra* note 108, 12-13;.

[265] *supra* note 257, para. 98.

[266] Davies B., *et al*., *supra* note 114, 19, 39.

[267] *Ibid.*, 39.

Although the nature of such episodes does not immediately reveal serious threats to fundamental rights and freedoms, the people misidentified have certainly confronted with an unpleasant experience. Yet, considering a possible expansion in the deployment of these systems, such an experience might potentially become an unfortunate part of our daily life. No matter how well-planned a hectic weekday or a relaxed day-off would be, anyone could be randomly stopped for further identifications by police officers due to an FRT *false positive* match.

In addition, it is not true that any false match ends with no significant harm. In fact, the error rate of FRSs has the tendency to be higher when the people involved belong to certain categories, as in the case of women or certain ethnic groups.[268] To bring a paradigmatic example, a false positive occurred in a US international airport and involving a person appearing of 'Middle Eastern' origins, ended with his detention by the FBI. The man lost his flight and after spending that night in a hotel, he was finally free to continue with his journey the following day.[269]

Other than the issues related to non-discrimination,[270] the several data protection infringements occurred in these episodes could generate serious doubts regarding the social trust the use of FRT by law enforcement deserves. Indeed, at this stage, rather than legitimate policing actions, such deployments appear more similar to arbitrary '*fishing expeditions*'.[271]

5.2 From test to test: the lack of adequate information, consent, and alternatives.

This section will allow exploring different issues which derive from the lack of adequate information provided by law enforcement on occasion of the test deployments

[268] Dushi D., *The use of facial recognition technology in EU law enforcement: Fundamental rights implications*, Global Campus (South East Europe) Policy Briefs 2020, 7.

[269] This episode is quoted in Introna L., *et al.*, *supra* note 107, 193 and in Introna L. *et al.*, *supra* note 112, 45.

[270] FRA, *supra* note 17, 27 *et seq.* Cf. Art. 21 CFR; Art. 14 ECHR and its Protocol No. 12.

[271] For this expression in its original context see Davies B., *et al*., *supra* note 114, 40.

considered. In this respect, according to a recently published study by the European Union Agency for Fundamental Rights (FRA), the provision of adequate information is a precondition for the effective exercise of the 'right to an effective remedy'.[272] However, the reflections brought in by the present analysis mainly relate to transparency, individual autonomy, and freedom of movement.

The specific processing of personal data within the pursuing of 'public security' excludes the element of the consent – otherwise essential.[273] Yet, Recital (26) LED mentions that '*[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing.*'[274] Then, with respect to 'particularly sensitive' categories of data, Recital (35) LED indicates strict *criteria* for their processing, and labels the mere consent of the data subjects as a legal ground not sufficient for doing so. In this regard, according to the European Data Protection Board (EDPB) entering an area marked as 'monitored' would not amount to *facta concludentia* clearly indicating the affirmative consent to the processing of personal data.[275]

Against this background, the information made available during the tests conducted in South Wales was limited to a notice saying '*Facial Recognition Fitted*' on the sides of the vans equipped with the cameras. The report shows that the operators provided with further information only the people involved in *false positive* matches or '*members of the public [who] stopped to look inside [the van], seemingly curious about the technology*'.[276] During the deployments by the London Metro Police, the degree of information provided was slightly higher as it involved '*uniformed officers to explain the public, leafleting and signage boards*' near the operative bases.[277]

[272] In this sense FRA, *supra* note 17, 31. Cf. Art. 47 CFR; Art. 6 ECHR.
[273] Cf. Recital (35) LED; Articles (6), (7), (9), GDPR and therein Chapter III – Sections 1.
[274] Recital (26) LED.
[275] EDPB, *supra* note 108, 12.
[276] Davies B., *et al*., *supra* note 114, 39.
[277] Fussey P. *et al*., *supra* note 238, 12, for further details see 92-100.

The practices just described do not seem in compliance with the indications provided by the LED. Moreover, in one case, the officers operating the tests showed aversion towards the implementation of information measures. In their opinion, the public notice of FRT deployments undermined their effectiveness since '*by the afternoon everyone in the neighbourhood knew about the trial*', thus implying that fewer people spontaneously passed by the monitored area.[278]

From the perspective of law enforcement, similar considerations seem to suggest that 'effective' uses of FRSs in public spaces are incompatible with adequate public information. Such a strict connection between allegedly higher levels of effectiveness and non-transparent FRT deployments seem to confirm the representation of such instruments as '*silent technologies*' given earlier in this chapter.[279]

While hoping for the implementation of more effective public notices about FRSs deployments in public spaces, one might wonder, what would the alternative be for all those citizens reluctant to be the object of facial scans. In this regard, the report on the trials conducted by the London Metro Police gives us an idea.

Whilst in one occasion the deviation necessary to proceed in the same direction avoiding the "recognition area" simply consisted in '*crossing the street*', in other cases, the '*walking detour'* would have required '*additional 18 minutes or paying to pass through the Underground Station ticket barriers*'.[280] Hence, it seems that – to date – the only possibilities to avoid facial scans in public spaces consist either in a "forced variable detour" or in the material impossibility to access certain areas. Similar trade-offs would be then more strongly enforced whenever elements of urban space, such as public lighting or the course of streets, were specifically designed or modified to guarantee better FRT working conditions.

Specific spatial configurations and other arrangements influencing '*movements patterns*' to guarantee a clearer view of peoples' face already exist in airports, sports

[278] Fussey P. *et al.*, *supra* note 238., 89.
[279] Introna L. *et al.*, *supra* note 107.
[280] Fussey P. *et al.*, *supra* note 238, 100.

arenas, casinos and other locations.[281] In this regard, according to the EDPB, when FRT works on '*anyone passing by*' a certain monitored area open to the public the access to that area should not be conditioned to '*the acceptance of the biometric processing*'; by contrast, alternative solutions not entailing the processing of biometrics should be available.[282]

From this perspective, it is important to reflect if '*[i]n societies that value freedom and autonomy, it is worth questioning whether the burden of requiring individuals to follow the route optimal for system performance rather than routes most efficacious for achieving their own goals is acceptable*'.[283]

Such considerations seem in strong connection with the right to free movement of individuals enshrined in Article 2 of Additional protocol N° 4 to the ECHR.[284] Yet, if it were possible to further interpret the last minute, on the fly, and undetailed modalities of information about FRSs deployments in public areas in light of the 'Unfair Commercial Practices Directive',[285] such methods would probably be labelled as 'Aggressive practices'. Indeed, in the context of provisions regarding the genuineness of the determination to take transactional decisions, this expression refers to the conclusion of a contract occurred in such circumstances which are '*likely to significantly impair the average consumer's freedom of choice or conduct with regard to the product and thereby causes him or is likely to cause him to take a transactional decision that he would not have taken otherwise.*'[286]

In this respect, an analogous reasoning could also be applied to all those interactions in the *digital world* which bind our access to various contents to the prior

[281] On these examples see Introna L. *et al.*, *supra* note 112, 20,

[282] EDPB, *supra* note 108, 17.

[283] Introna L. *et al.*, *supra* note 112, 46.

[284] Venice Commission, *supra* note 240, 9.; Azria S. and Wickert F., *Facial Recognition: Current Situation and Challenges*, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data [T-PD(2019)05rev], 2019, 17.

[285] Directive 2005/29/EC of the European Parliament and of the Council of 11th May 2005 concerning unfair business-to-consumer commercial practices in the internal market as amended by the Directive (EU) 2019/2161 of the European Parliament and of the Council of 27th November 2019.

[286] Section 2, Directive 2005/29/EC.

agreement to Terms of Service, Cookies and Privacy policies. One might argue that such information or consent-based schemes do not appear sufficient (1) to make many consumers, users, and "digital citizens", aware of their rights (2) to effectively protect data protection and privacy rights. Such failures occur whenever a consent-based transactional decision is blindly taken just to access to a service instead of being "excluded" from it.

Now, let us imagine that it is an ordinary day and we are on our way home when we suddenly notice a complex signage announcing the deployment of FRT: other than the time loss of a detour, the only alternative to the surrender of our rights would be the defeat of our individual autonomy.

5.3 Modern technologies and the right to exercise rights.

While the last section ended with a few considerations about the necessity to be aware of our rights, the urgency to exercise them and avoid their gradual erosion in a fast-changing world, the present section opens with the intersection among the use of FRSs and the right to peacefully gather with others and, if necessary, to protest for a common cause.

On April 2015, the city of Baltimore (Maryland, US) was deeply touched by Freddie Grey's death. He, a 25-years-old Afro-American, lost his life a week after being hospitalised for spinal injuries related to his arrest by the Baltimore police.[287]

Since the day of the violent arrest – documented by video-recordings of fortuitous witnesses – pacific demonstrations against '*excessive use of force*' have flooded the streets. When the death of the boy was announced, the situation violently escalated.[288]

The local authorities progressively restored the order with the help of a tech-tool from the company Geofeedia. By mining protestors' social media data, this

[287] *Freddie Gray's death in police custody - what we know*, BBC NEWS, 23 May 2016, available at https://www.bbc.com/news/world-us-canada-32400497.

[288] *Ibid.*

software provided law enforcement authorities with '*real-time maps*' about '*activity in protest areas*'.[289] The deployment of this tool provoked different reactions. Whilst the company stressed that '*[i]n some cases, police officers were even able to run social media photos through facial recognition technology to discover rioters with outstanding warrants and arrest them directly from the crowd*',[290] the social media platforms involved sent to the company cease-and-desist letters claiming that such uses of users' data are against their policies.[291] Other concerns were raised by all those people who, pacifically joining the demonstrations, were scared that the deployment of FRT could have associated them with the actions of violent protesters.

This is the case of the Rep. and Chairperson of the House of Representatives Oversight Committee Elijah Cummings. In fact, he was among those '*community leaders marching in peace and trying to calm down residents*', who without their knowledge had been visible to the FRSs used to detect those committing crimes amid the protests.[292]

At the time of writing, the tragic death of George Floyd on May 25, 2020 and the chain of events that followed make an analysis on similar episodes extremely topical.[293] In the first place, such tragedies invite to reflect about the urgency of concrete forms of social justice and substantial applications of the 'equal protection principle', as the one emerging from the Fourteenth Amendment of 1868 to the US

---

[289] Brandom R., *Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors*, The Verge, 11 Oct. 2016, available at https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api.

[290] Geofeedia, *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, Case Study: Baltimore County PD,

[291] Brandom R., *supra* note 289.

[292] See *Fix bias in facial recognition technology*, The Baltimore Sun, published on 05 Jun. 2019. See also The US House Committee on Oversight and Reform, Hearing '*Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*', *supra* note 175.

[293] Hill E., Tiefenthäler A., Triebert C., Drew J., Willis H. and Stein R., *How George Floyd Was Killed in Police Custody*, The New York Times, 19 June 2020, available at https://www.nytimes.com/2020/05/31/us/george-floyd-investigation.html; Bryson Taylor D., *George Floyd Protests: A Timeline*, The New York Times, 18 June 2020, available at https://www.nytimes.com/article/george-floyd-protests-timeline.html.

Constitution. According to it, any State shall not '*deny to any person within its jurisdiction the equal protection of the laws*'.[294] Moreover, both technological advancements and recent protests in the US have also prompted the UN Human Rights Committee to issue, through General comment No. 37 (July 27, 2020), a comprehensive interpretation of the 'Right to peaceful assembly' as enshrined in Article 21 ICCPR.[295]

With this in mind, the rapid expansion of FRT and its deployment to suppress demonstrations appear alarming. As the example of Baltimore demonstrates, '*being in the wrong place at the wrong time*' implies the collection, storing and clustering of personal data within those of other people, perhaps involved in "suspect activities" different from a protest of political nature.[296]

Considering the principles and provisions already mentioned throughout this Chapter, under a European perspective, this controversial episode invites to a deeper reflection about the use of advanced technologies – including facial recognition – to monitor and track people taking part in protest and demonstrations. In doing so, the jurisprudence of the ECtHR provides interesting insights, as striking a right balance between the right to freedom assembly and the protection of public order is not an easy task.

The heading and wording of Article 11 ECHR[297] limit the scope of protection just to assemblies qualified as 'peaceful'. Therefore, only gatherings of people for the purpose of contributing '*to a public debate on matters of social importance*', whose participants have '*non-violent intentions*' would be covered.[298] In this regard, the indiscriminate gathering of data occurred through video recording and facial recognition in Baltimore, other than in contrast with the '*Marper* doctrine' and the legal instruments prescribing the distinction of the data processing of different categories of

[294] Amendment XIV Section 1 of the U.S. Constitution.
[295] UN Human Rights Committee, General comment No. 37 'Article 21', UN Doc. CCPR/C/GC/37, July 27, 2020.
[296] Lynch J., *supra* note 112, 7.
[297] As well as those of Arts. 21 ICCPR and 12 CFR.
[298] Broeksteeg H., *supra* note 127, 818.

persons, could also be considered against the principles in *Ezelin v. France*. Here, the Court, while evaluating the 'necessity in a democratic society' of the disciplinary measures taken against an avocat participating to a demonstration, stated that none should be censured for participating in a peaceful assembly '*that had not been prohibited […] as long as the person concerned does not himself commit any reprehensible act*'.[299]

Yet, under a 'public order perspective', many would deny the legitimacy of spontaneous demonstrations originated as an immediate response to certain events arguing the necessity for prior notifications, authorisations or other forms of sanction by public authorities. On this point, the ECtHR recognises that '*in special circumstances when an immediate response, in the form of a demonstration, to a political event might be justified, a decision to disband the ensuing, peaceful assembly solely because of the absence of the requisite prior notice, without any illegal conduct by the participants, amounts to a disproportionate restriction on freedom of peaceful assembly*'.[300] This doctrine is therefore intended as a form of justified derogation from the requirement of prior notification present in many jurisdictions when spontaneous expressions of public dissent appear justified by the circumstances of the case.[301]

Moving to the positive obligations related to the right of peaceful assembly, these involve the adoption of adequate measures aiming at guaranteeing the peaceful nature of the demonstrations through the protection of the participants against *e.g.* groups promoting opinions in contrast with those upheld.[302] Additionally, in the Court's opinion, similar safeguards also create a more favourable environment for the public expression of ideas. Participants would '*be able to hold the demonstration without having fear that they will be subjected to physical violence by their opponents*',

[299] ECtHR, *Ezelin v. France*, 11800/85, 26 Apr. 1991, para. 53.

[300] ECtHR, *Bukta and others v. Hungary*, 25691/04, 17 July 2007, para. 36; *Frumkin v. Russia*, 74568/12, 5 January 2016, para. 97. See also 16; 70 *et seq.*

[301] Broeksteeg H., *supra* note 127, 819.

[302] *Ibid.*, 821.

since the apprehension given by that circumstances could produce *chilling effects* towards the public free expression of opinions.[303]

In light of these elements, the same line of reasoning could be applied *mutatis mutandis* to the fear generated (1) by the use of violence from public authorities, (2) and by the indiscriminate deployment of enhanced forms of surveillance during protests or demonstrations. In this sense, the 'Guidelines on Freedom of Peaceful Assembly' jointly published by the CoE 'Commission for democracy through law' (Venice Commission) and the OSCE 'Office for democratic institutions and human rights' (ODIHR) specify that the resort to image recording and identifications through FRT should take place in presence of adequate safeguards against abuses, and when justified by the '*reasonable suspicion of imminent criminal behaviour*'.[304] Conversely, any record and retention of data, or identification of people not related to unlawful conducts, despite occurring in public spaces, may amount to a violation of the right to privacy.[305] In this respect, the UN Human Rights Committee General comment No.34 explicitly referred to the use of facial recognition.[306]

The results of an unreasonable reliance on the intelligence gathered through these forms of mass surveillance could lead to the abusive use of more intrusive investigative powers, hence generating iniquitous actions of targeted surveillance '*– often [affecting] journalists, activists, opposition figures, critics and others exercising their right to freedom of expression*'[307] or discouraging their spontaneous participation in such public events for fear of reprisals.[308]

However, the combination of CCTV and machine learning is not limited to identifications in public places or during protests through FRSs, as such technologies are increasingly spreading to other contexts *e.g.* to distinguish "normal" from

[303] ECtHR, *Plattform Arzte fur das Leben v. Austria*, 10126/82, 21 June 1988, para. 32; see also General comment No. 34, *supra* note 276.

[304] Venice Commission and ODIHR, *Guidelines on freedom of peaceful assembly (3rd Edition)*, Strasbourg/Warsaw, [CDL-AD(2019)017], 2019, para. 172.

[305] *Ibid.*, 67 and note 334.

[306] General comment No. 34, *supra* note 276, para 62.

[307] Kaye D. *Surveillance and human rights*, *supra* note 204, para. 1.

[308] General comment No. 34, *supra* note 276, para 33.

"suspicious" behaviours, thus spotting '*if you are a terrorist or a criminal – before you even commit a crime*'. For instance, in "high-risk places" as airports, the indicators taken into account in these circumstances can include '*"exaggerated yawning"; excessive "grooming gestures"; "fast eye blink rate"; a lack of eye contact; "excessive fidgeting, clock watching, head-turning, shuffling feet, leg shaking"*'.[309] Similar forms of behavioural detection are also deployed in the UK to predict '*potential disorders*' before they even materialise.[310]

Yet, the pursuit of enhanced levels of 'public safety' through *silent technologies* operating through '*covert, remote, and mass capture*' of biometric data[311] appears prone to abuses and easily exploitable for advanced levels of oppression.[312]

With these in mind, the coincident run towards more breadth surveillance infrastructures appears particularly frightening.

5.4 Towards a growing infrastructure. Pervasive surveillance and chilling effects.

In the ranking of the most "camera-surveilled" cities in the world, London and Atlanta stand out as the only cities 'outside of China' within the 'top ten', whilst also Berlin and Moscow appear in the 'top twenty'.[313]

Since late 2017, Moscow declares on its official website a CCTV real-time facial recognition network covering the '*95 percent of residential buildings*', therefore

[309] Ackerman S., *TSA screening program risks racial profiling amid shaky science – study*, The Guardian, 8 Feb. 2017, available at https://www.theguardian.com/us-news/2017/feb/08/tsa-screening-racial-religious-profiling-aclu-study.

[310] Wilson D. *et al.*, *supra* note 95, 82-83. See also Skogan W. G., *The future of CCTV*, Criminology & Public Policy, 18(1), 2019, 161-166, 162

[311] Lynch J., *supra* note 112, 7.

[312] Hartzog W., *Facial Recognition Is the Perfect Tool for Oppression*, Medium, published on 2 Aug. 2018, available at https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

[313] Bischoff P., *Surveillance camera statistics: which cities have the most CCTV cameras?*, Comparitech, 15 Aug. 2019, available at https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

proclaiming to have '*one of the world's largest CCTV systems with face recognition*'.[314] What is more, thanks to a special agreement, citizens are able to connect their private security systems to the city's infrastructure.[315] This network expansion guarantees public authorities the "virtual access" to private spaces,[316] which, in democratic States respectful of the rule of law, would be inscrutable without adequate judicial supervision. Still, the city indicates as a priority '*to maintain a balance between privacy and security*' thanks to rigid policies in compliance with fundamental rights standards.[317]

To date, the growth of the surveillance network in Moscow has spread like wildfire. Indeed, in 2019 conspicuous investments were made for the purchase of additional resources.[318] Approximately one year later that news, a case was submitted before the Tverskoy District Court of Moscow: the applicants argued that FRSs have been unlawfully deployed to monitor protests, demonstrations and other assemblies where '*bulk […] collection, storage and analysis of sensitive personal data [took place] without individualized reasonable suspicion*.[319] In March 2020, such

---

[314] *Moscow has one of the world's largest CCTV systems with face recognition*, mos.ru – Moscow Mayor official website, 29 Sep. 2017, available at https://www.mos.ru/en/news/item/30105073/.

[315] *Ibid.*

[316] Unfortunately, recent news report that illegal '*access to Moscow's surveillance cameras – and their facial recognition technology – is being sold on the black market*', see Korelina O., *As Moscow's facial recognition system activates, journalists find access to it for sale on the black market*, Meduza, 5 Dec. 2019, available at https://meduza.io/en/feature/2019/12/06/as-moscow-s-facial-recognition-system-activates-journalists-find-access-to-it-for-sale-on-the-black-market.

[317] Moscow Mayor official website, *supra* note 314.

[318] *Moscow to Deploy Facial-Recognition Tech at Rallies*, The Moscow Times, published on 6 Sep. 2019, available at https://www.themoscowtimes.com/2019/09/06/moscow-to-deploy-facial-recognition-tech-at-rallies-a67174; Brewster T., *Remember Find Face? The Russian Facial Recognition Company Just Turned On A Massive, Multimillion-Dollar Moscow Surveillance System*, Forbes, 29 Jan. 2020, available at https://www.forbes.com/sites/thomasbrewster/2020/01/29/findface-rolls-out-huge-facial-recognition-surveillance-in-moscow-russia/.

[319] *Russia: Intrusive facial recognition technology must not be used to crackdown on protests*, Amnesty International, 31 Jan. 2020, available at https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/; *Russia's use of facial recognition*

deployments have been confirmed during the court proceeding, yet the District Court ruled such measures as legitimate.[320]As a result, the ECtHR has received its '*first complaint about facial recognition systems*'[321] since the applicants claim the measures at issue in contrast with several ECHR provisions as Articles 8, 11, 13, and 14 ECHR.[322]

Going beyond specific cases such as the last mentioned, the possibility of a real-time 24/7 FRT usage would not only allow to '*recreate a suspect's movements*'[323] or '*to support investigators searching video evidence in the aftermath of an incident*'.[324] It would also mean a "system of total surveillance", as everyone's identity would be continuously checked in an 'ideal open-air checkpoint'.[325] In such a context, any expectation of anonymity or not to be associated with certain places, persons, habits or services would simply be lost.

Moving from *Kopp v. Switzerland*,[326] where surveillance itself – regardless of whether the information gathered had been used in the prosecution of the applicant or not – had been considered amounting to an interference with Article 8 ECHR,[327] such enhanced forms of control create particular concerns with regard to all those cases where the association with certain places would give private insights about '*individual's political, religious or social views, […] or activities (e.g., churches, abortion clinics, etc.)'*.[328] If used to infer similar information, the processing of video

challenged in court, BBC News, 31 Jan. 2020, available at https://www.bbc.com/news/technology-51324841.

[320] Zlobina A., *Moscow's Use of Facial Recognition Technology Challanged*, Human Rights Watch, 8 July, 2020, available at https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged.

[321] *ECHR receives first complaint about facial recognition system in Moscow*, TASS, 6 July, 2020, available at https://tass.com/society/1175141.

[322] *Ibid.*

[323] *Moscow has one of the world's largest CCTV systems with face recognition, supra* note 314.

[324] THALES, *supra* note 112.

[325] Fussey P. *et al.*, *supra* note 238, 20.

[326] ECtHR, 23224/94, 25 March 1998, para. 53.

[327] Similarly, ECtHR, *Amann v. Switzerland*, 27798/95, 16 February 2000, para. 69.

[328] *Privacy Impact Assessment Report*, *supra* note 115, 19.

footages would fall within the processing of special categories of data.[329] In light of Article 10 LED, such processes should take place '*only where strictly necessary*', with adequate safeguards put in place, and only '*where authorised by Union or Member State law*', '*to protect the vital interests of the data subject or of another natural person*' or whenever the processing relates to data '*manifestly made public by the data subject*'.[330]

In this regard, the voluntary surrender to rights related to private spheres and data protection are deduced neither by the exposure 'to others' in public spaces,[331] nor by '*[t]he mere fact of entering into the range of [a] camera*.[332] In *Niemietz v. Germany*, the ECtHR, while labelling a notion of private life related just to '*inner cicles*' as '*too restrictive*', made clear the relevance of private life also in public spheres.[333] Similarly, in *Bigaeva v. Greece* the Court recognised the importance '*to form and develop relationships with others' as part of 'the right to live a "social private life", that is the possibility for an individual to develop his or her social identity*'.[334]

Consistent principles have also been recalled in *Unuz v. Germany*, where, in the context of surveillance for the investigations of *serious crimes*, the Court reaffirmed the existence of '*reasonable expectations*' of privacy also in public spaces and considered the monitoring through technological means – specifically the '*systematic or permanent record of video materials*' – of particular concern.[335]

From a different angle, such invasive surveillance practices have the potential to turn upside down our lives upsetting the existent *equilibrium* between governors and governed, democratic guarantees and the rule of law.[336] Considering the deterrence of socially undesirable behaviours pursued by criminal law, individuals are expected to forge their decisions and adjust their conducts by pondering the 'expected value'

[329] EDPB, *supra* note 108, 14.
[330] Article 10 LED.
[331] Venice Commission, *supra* note 240, 7.
[332] EDPB, *supra* note 108, 15.
[333] EctHR, 13710/88, 16 December 1992, para. 29.
[334] EctHR, 26713/05, 28 August 2009, para. 22.
[335] ECtHR, 35623/05, paras. 43 *et seq.*
[336] Richards N. M., *The dangers of surveillance*, Harv. L. Rev., 126, 2012, 1934 *et seq.*

originating from a certain action with the certainty of the detection, and the consequent punishment of an illegal action.[337] Yet, when it comes to hi-tech surveillance in public spaces, the conclusion of analogous calculations may put '*an additional pressure on the individual to prevent the detection of what might be perceived as anomalies*',[338] including *chilling effects* towards the exercise of lawful actions, even when amounting to protected civil rights and liberties. Indeed, '*the mere possibility of surveillance has the potential to make people feel extremely uncomfortable, [and to] cause people to alter their behavior, and lead to self-censorship and inhibition*'.[339] Ultimately, by enabling unprecedented forms of social control, FRT may subtly restrict the enjoyment of all those spheres related to '*human development, […] autonomy, creativity, [and] social identity experimentation*'.[340]

This kind of consequences may endanger the community life and the individuals' participation in all those public debates involving religious, political, and other beliefs in contrast with those of a well-established majority. Eventually, every aspect of our personality might have to be repressed because potentially appreciable as a deviance from the dominant current of thought.

Whilst phenomena of data mining and online surveillance to find 'suspect patterns of behaviour' and identify individuals worthy of further scrutiny, turned out to be an effective method to '*suppress legitimate political dissent or monitor individuals simply because of their political beliefs, […] or affiliations*',[341] the newest advancements in real-time video-surveillance take hold embedded in an all-round technological *apparatus* that assumes the dimension of an '*urban ecosystem*'.[342] The more our cities become '*smart*' the more the human body is '*permanently "on*

[337] Cf. Stoycheff E., Liu J., Xu K., & Wibowo K, *Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects*, New media & society, 21(3), 602-619, 605. See *i.a.* Piza E. L., Welsh B. C., Farrington D. P. & Thomas A. L., *CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis*, Criminology & Public Policy, 18(1), 135-159, 137.

[338] EDPB, *supra* note 108, 4.

[339] *Privacy Impact Assessment Report*, *supra* note 115, 2.

[340] Büchi M., *et al.*, *supra* note 101, 2.

[341] Stoycheff E., *et al.*, *supra* note 337, 604.

[342] Skogan W. G., *supra* note 310, 165.

grid"".[343] When our facial traits and our identity come to be promptly detected and translated into *mathematic artifacts*, there is no more physical reality which is not mined.[344]

6. Upholding the individual and collective flourishing through human dignity. Conclusions.

The analysis of the topics widely treated in this Chapter, and particularly the considerations at the end of the previous section urge to reflect on the numerous issues related to the use of FRT by law enforcement. Among different approaches, the standpoint here adopted aims at bringing back to centre the preminence of human beings respect to the oppressive potential of an over-taking technological environment. Indeed, an analysis too much focused on advanced forms of crime detection and control could risk losing sight of aspects crucially relevant in the context of a dissertation which seeks to "frame" the use of FRT from a human rights perspective.

Recalling the UDHR, as the ideological bedrock of the European systems of human rights protection,[345] an interesting observation can be made by analysing its Preamble. There, '*the inherent dignity […] of all the members of the human family*' emerges as the essential foundation for the pursuit of other fundamental values such as freedom, *justice*, and peace. Accordingly, human dignity does not appear to be conditioned or subordinated in any way to other social goals, as the fight against crime or the achievement of increased levels of "security".[346] Similarly, in the sector-specific context of the 'Oviedo Convention' for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine, its Article

[343] Wilson D., *et al.*, *supra* note 95, 82.

[344] For the concept of 'reality mining' see Zuboff S., *supra* note 10, 84, and the bibliography therewith referenced.

[345] In this sense see the reference in the preamble of the ECHR and the 'Explanatory Note' on Article 1 CFR, see Dupré C., *Human Dignity*, in *The EU Charter*, *supra* note 124, 3.

[346] UDHR, Preamble.

1 recalls the protection of '*dignity and identity of all human beings*', while Article 2 affirms the primacy of the human being '*over the sole interest of society*'.[347]

With a specific emphasis on the European human rights framework,[348] if in EU primary law, the respect for human dignity stands out as the first right enshrined in the CFR as well as, the first of the 'European foundational values' consecrated in Article 2 TEU,[349] the ECHR makes extremely limited reference to human dignity.[350] Yet, it is extensively used in the ECtHR case-law.[351] In fact, although to describe the essence of such a concept is a particularly complex task,[352] a few essential elements on it can be *a contrario* deduced from the ECtHR jurisprudence which, *i.a.* in the context of Article 3, considered an action as 'degrading' when it '*humiliates or debases an individual, showing a lack of respect for, or diminishing, his or her human dignity'*.[353]

Despite a similar correlation might *per se* appear radical, if considering (1) the 'reduction' of the human identity to a *mathematic artifact* as a form of objectification of the human being;[354] (2) the effects on self-determination of a constant and intrusive technological gaze, which may even compromise the spontaneous exercise of the fundamental rights and freedoms founding liberal democracies; it may be argued that elements such as *humiliation*, *debasement*, and *lack of respect for human dignity* could be relevant in the evaluation of the effects generated by more and more intrusive uses of FRT.

---

[347] Oviedo Convention (ETS No. 164).

[348] *Supra*, Chapter II., Section '*2. The Human Rights Protection in Europe'.*

[349] Cf. Art. 1 CFR; Art. 2 TEU.

[350] Heselhaus S. & Hemsley R., *Human Dignity and the European Convention on Human Rights*, in Becchi P. & Mathis K. (Eds.), *Handbook of Human Dignity in Europe*, Springer International Publishing, 2019, 970 *et seq.*

[351] *Ibid.*

[352] *i.a.* Carrozza, P. G., *Human dignity*. In Shelton D. (Ed.), *The Oxford handbook of international human rights law*. Oxford University Press, 2013; Becchi P. & Mathis K., *supra* note 331.

[353] ECtHR, *MSS v Belgium and Greece*, 30696/09, 21 January 2011, para 220 and *Pretty v. U.K.*, 2346/02, 29 July 2002, para 52.

[354] In terms of '*treating individuals as objects rather than as moral subjects*' also the CoE Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT), *A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework*, published on 9 Nov. 2018, [MSI-AUT(2018)05], 6.

The resort to similar arguments is then not merely abstract, since also the European Union Agency for Fundamental Rights (FRA) has recently stressed that

> *[p]eople may feel uncomfortable going to public places under surveillance. They may change their behaviour, withdrawing from social life, not visiting central places under surveillance, avoiding train stations or declining to attend cultural, social or sports events. Depending on the extent to which live facial recognition technologies are applied, the impact on what people may perceive as surveillance technologies on their lives may be so significant as to affect their capacity to live a dignified life.*[355]

It is interesting to note how from this excerpt individual privacy and self-determination transpire as fundamental elements for the fulfilment of a '*dignified life*'. In this regard, the intersection among these concepts originally developed within the jurisprudence of the ECtHR with respect to Article 8. Indeed, over time, the 'right to respect for private and family life' expanded from its original form of '*negative freedom in vertical relations'* reaching a level of protection which encompasses also '*positive freedoms*'.[356] Among these, the possibility to freely form and express opinions and to fully develop one's personal identity thanks to the interactions with others, which constitute the enabling environment for the 'human flourishing'.[357]

From this angle, an important lesson could be learned from the use of this ideologically powerful concept made by the ECtHR to '*strengthen […] the centrality and importance of the right in question and limit […] possible exceptions or limitations to that right*'.[358] In our case, human dignity could be used to bolster the right to freely act and exercise rights, or develop fundamental spheres of our personality – also in public spaces, through the protection of the rights to private life, to personal data and

[355] FRA, *supra* note 17, 20. This argument is also used in Jakubowska E. *et al.*, *supra* note 93, 22-23.
[356] van der Sloot, *supra* note 124.
[357] *Ibid.*
[358] Carrozza, P. G., *supra* note 352.

freedom of assembly against excessive interferences driven by the pursuit of public security.

Hence, the foundational position of human dignity, as essential 'mother right' from which all human rights stem,[359] would allow to bring '*individuals at the centre […] protecting them in their relations with power*'.[360] Viewed in this way, also the Kantian moral imperative which sees humans to be always treated as an end instead of being *e.g.* manipulated as objects to govern[361] through oppressive security policies would be respected.

[359] *i.a.* Barak, A., *Human dignity: the constitutional value and the constitutional right*, Cambridge University Press, 2015, 156-169.

[360] Dupré C., *supra* 345, 7.

[361] The renowned reference is to Kant I., *Critique of practical reason and other works on the theory of ethics*, Barnes & Noble Publishing, 2004.

CHAPTER IV.

The rule of law and the social legitimacy of Facial Recognition Technology.

1. The improper use of an imperfect technology, and its risks.

In light of the noteworthy interests put at stake by the deployment of FRT by law enforcement, it seems now appropriate to further deepen the consequences deriving from the reliability of those systems and their practical use by the long arm of the law.

It is intuitive, the highly-sensitive task to associate a "criminal identity" to a common citizen, enjoying the basic right to be presumed innocent until proven guilty, could not be entrusted to systems that, despite modern, misinterpret images in ways that not even the least brilliant of the (human) observers would do. Yet, even machines utilising advanced computer vision techniques may confuse the picture of a turtle for that of a gun.[362] In the context of law enforcement, it is not too hard to imagine which dramatic consequences would be caused, if such a mistake could automatically trigger follow-up actions not supervised by well-trained professionals. In the same manner, although assisted by modern technologies, also the identification of suspects is not a simple task. It involves the interaction among different elements, such as the quality of the hardware utilised, its performances when coupled with a certain software, the results of the processing, the judgement and decisions of the operators involved.[363]

[362] Conner-Simons A., *Fooling Neural Networks w/3D-Printed Objects*, MIT Computer Science & Artificial Intelligence Lab, 2 Nov. 2017, available at https://www.csail.mit.edu/news/fooling-neural-networks-w3d-printed-objects; as referenced in Raso F. *et al.*, *supra* note 22, 11.

[363] Davies B., *supra* note 114, 40.

Undoubtedly, as in every visual identification task, the best accuracy is "guaranteed" by images taken with high-definition devices, when the "environmental factors" such as lightening, facial exposure *etc.* are under control. In this sense, '*facial images, portraits, or mug shots*' must be preferred.[364] By contrast, FRSs underperform when confronted with low-quality templates, or images not taken in technically ideal conditions. What is more, among the factors affecting a search outcome, also the inherent characteristics of the subject portrayed play an important role. As a matter of fact, FRT reacts differently to characteristics as gender and age, physiognomy deriving from diseases or disabilities, and other elements typical of certain ethnic groups – *e.g.* the tone of the skin[365] or its texture.[366] The potential negative repercussions affecting those belonging to the most affected 'types' exposed FRSs to strong criticisms about such discriminatory levels of accuracy.[367]

Yet, an investigation carried out by the New York Police Department (NYPD) shows how technical shortcomings are far from being overcome through diligent and trustworthy uses of FRT. Indeed, in April 2017, when a NYPD facial recognition search proved unsuccessful, the officers involved showed great zeal and determination. On that occasion, whilst the low-quality CCTV frame of a shoplifter stealing some beers

---

[364] *i.a.* FRA, *supra* note 17, 8. For further technical details about quality assessment criteria see Introna L. *et al.*, *supra* note 112, 18. According to Davies B., *et al.*, *supra* note 114, 17, the ability of the system '*to detect a face'* depends on the settings related to '*the number of pixels needed between the two pupils of the eyes […] This is affected by several factors including resolution of the image, distance from the camera to the subject, and level of optical zoom*'. By contrast, '*[p]oor quality probe images due to unpredictable light and shadows in outdoor scenes, unpredictable facial orientation, and "noise" from cluttered backgrounds make it difficult for an FRS in the first place to even pick out faces in the images*', see Introna L. *et al.*, *supra* note 112, 20.

[365] *Ibid.*

[366] Garvie C. *et al.*, *supra* note 171, 9.

[367] *Ibid.*, 53; Girasa R., *supra* note 23, 115. More broadly on the theme of 'algorithmic discrimination' in criminal justice see Angwin J., Larson J., Mattu S. and Kirchner L., *Machine Bias*, ProPublica, 23 May 2016, available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. About discrimination in criminal justice see The Lammy Review, *An independent review into the treatment of, and outcomes for, Black, Asian and Minority Ethnic individuals in the Criminal Justice System*, 2017, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643001/lammy-review-final-report.pdf.

from a store did not allow any 'identification match',[368] an officer noticed a striking resemblance between the *highly pixelated* image of the suspect and the American actor Woody Harrelson. Once a *high-quality* picture of the actor had been downloaded from the internet and uploaded to the FRS – "there you have it!". This time, the image search conducted '– *not to Harrelson but to the suspect whose photo had produced no possible hints*'.[369]

If on the one hand, this case might provoke admiration for the enthusiasm demonstrated by the NYPD while carrying out its duties, the fact that criminal investigations result based on luck or, even worse, on a clear *technical error* of the FRSs utilised should generate significant concerns.

In this sense, a "facial search" for a specific biometric template can lead to two opposite outcomes: (1) there is no match as the algorithm does not recognise any relationship with the reference data contained in the given database; (2) there is a match since the system recognises the 'unique traits' extracted by the uploaded sample in one or more images within the reference gallery. To be more specific, the outcome of a search is not expressed in sharp "positive-or-negative" binary terms, as the results proposed by the system consist of a set of the most probable matches.[370] Yet, in such circumstances, the range of "proposed results" is not the only variable present. Indeed, one should bear in mind that the system may be wrong reporting *false-positive* or *false-negative* results. On this point, it is worth specifying that, when the system recognises the correct person in the database, we have a *true-positive* match. Conversely, when it does not detect any match because there is not an image in the gallery corresponding to that person, we have a *true-negative*. Moreover, we can have phenomena of *false-*

[368] NYPD, Real Time Crime Center Facial Identification Section (FIS), presentation by Detective Markiewicz (Sept. 17, 2018) (notes on file with author), as referenced in Garvie C., *Garbage in, garbage out. Face Recognition on Flawed Data*, Georgetown University, Center on Privacy & Technology, May 2019, available at https://www.flawedfacedata.com/#footnote1_sbqip7e.

[369] *Ibid*.

[370] Garvie C., *supra* note 368, 9. For further information on the '*ranked list of possible matches'* see Introna L. *et al*., *supra* note 112, 12.; see also FRA, *supra* note 17, 9. In Davies B. *et al*., *supra* note 114, 12, this process is described as a '*"gradient score" that indicates the probability of two people being the same*'.

positive and *false-negative* whenever the probe image is matched with an incorrect identity in the gallery, or the system does not detect any match despite the suspect is actually in the given dataset.[371]

The incidence of false-positive and false-negative matches is important data. For instance, while performing a *verification* task to unlock a personal device, a *higher false-negative rate* could be desirable. Although it can be frustrating, having to make a few attempts to access to a smartphone, it is a synonym of security. In such circumstances, it is unlikely that the device will be easily unlocked by an impostor. The other way round, when discussing the use of FRT by law enforcement, a *high false-positive rate* might imply a misidentification, *i.e.* bringing an innocent in the middle of a criminal investigation.[372]

After this brief technical digression about the possible outcome of facial recognition searches, it will be probably clearer that the (mis)identification process and the consequent arrest of the "New York beer thief" was nothing but the *aware* and *accepted* result of an *induced false-positive* identification.

Other examples of FRT "creative uses" include searches run using hand-made forensic sketches, or even actual patchworks where facial features are digitally removed, created and inserted, in order to increase the possibility of a "conclusive search".[373] On top of that, the landscape of censurable uses of FRT not only encompasses authorities, perhaps, excessively eager to conduct productive investigations, but it also includes cases where the misuse of powerful technological devices has nothing in common with their original purposes.

---

[371] For further details on FRT functioning, extensively Introna L. *et al.*, *supra* note 112, particularly on the array of possible outcomes of each facial recognition task, 11-13, and the diagrams therein. On the notions of '*false positives and false negatives*' also Davies B., *et al.*, *supra* note 114, 13; FRA, *supra* note 17, 9, where it is specified that the modification of the '*probability threshold*' for a match implies '*a trade-off between false positives and false negatives*'.

[372] Similarly, Lynch J., *supra* note 112, 6.

[373] Garvie C., *supra* note 368.

Several inquiries, mainly conducted in the US, showed widespread abuses of surveillance tools and sensitive databases to unlawfully obtain information for private ends. The case history about such secondary uses includes monitoring of partners or spouses, the stalking of *'ex-girlfriends'* and searches for personal data of women *'found attractive*'.[374] The same *function creep* has been shown in the UK where it is reported that *'mostly male operators used [...] cameras to spy on women*'.[375]

In light of such arbitrary practices, against any kind of professional ethic, the concerns hitherto raised by instruments as *Clearview* or by the capabilities of live facial recognition should sound even more alarming. Indeed, the litmus test encompassing the strong inconsistency of FRT with several fundamental rights and freedoms, its technical shortcomings, and the abuses in its use, does not seem to turn out positively.

2. Social trust and the rule of law. The role of procedural justice.

The final considerations of the previous section may result more founded after the following reflections. Indeed, if it is true that distinctive facial traits are unique, and only a few factors as ageing, massive use of cosmetics, significant effects of drug abuse or smoking, and plastic surgery can modify them,[376] one might wonder how it is possible that law enforcement agencies consciously base their activities on unscrupulous uses of FRT, as those previously emerged. And again, what is the chance that asking to FRSs to search for the forensic sketch of an alleged perpetrator, the result of that search will be accurate? Such doubts could be shared by all those individuals, who would expect rigorous methods and elevate standards in the performance of highly sensitive tasks performed by law enforcement. Particularly, when it comes to criminal investigations, coercive State powers and the legitimate monopoly in the use of force.

---

[374] Lynch J., *supra* note 112, 11-12 and the content of the endnotes there mentioned.
[375] *Ibid.*
[376] See the INTERPOL's page on Facial Recognition available at https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition.

This might be the case of Amara K. Majeed. In April 2019, this student from Brown University in Providence (Rhode Island, US) discovered that her face had been associated to the Sri Lankan 'Easter bombings' attack, where over 250 victims lost their lives.[377] In fact, the FRS used by the Sri Lankan authorities coupled Amara's image with the identity of the possible accomplice of that heinous crime; the ISIS-affiliate Abdul Cader Fathima Khadhiya.[378] Albeit the authorities promptly apologised for the incident, the young student received death threats due to that false identification.[379] She and her family's lives were in danger.

By analysing the "anatomy" of this episode a clear picture of the disruptive potential of FRT incautious uses emerges. In this case, an error, a butterfly's flap – as someone would say[380] – exposed to danger the life of the young Amara and several members of her family, both in the US and in Sri Lanka. As a matter of facts, all the innocent people involved in this episode have suddenly tumbled into a dangerous scenario encompassing violent political crimes, religious fundamentalism, and the intersection of ethnic and religious minorities. In this sense, it would be very distressing to picture ourselves in the shoes of a young Muslim and feminist activist[381] identified

[377] Specia M., *American Student Misidentified as Sri Lanka Suspect Faces Backlash*, The New York Times, 26 Apr. 2019, available at https://www.nytimes.com/2019/04/26/world/asia/sri-lanka-brown-student.html; Fox J. C, *Brown University student mistakenly identified as Sri Lanka bombing suspect*, The Boston Globe, 28 Apr. 2019, available at https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html.

[378] *US woman wrongly identified as Sri Lanka attack suspect*, BBC NEWS, published on 26 Apr. 2019, available at https://www.bbc.com/news/world-asia-48061811; Buolamwini J., *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties (written testimony)*, United States House Committee on Oversight and Government Reform, 22 May 2019, 7, available at https://docs.house.gov/meetings/GO/GO00/20190522/109521/HHRG-116-GO00-Wstate-BuolamwiniJ-20190522.pdf.

[379] *Ibid.*

[380] The popular concept according to which even a butterfly's flap could cause huge consequences was originally established in the field of meteorology, Lorenz E., *Predictability: does the flap of a butterfly's wing in Brazil set off a tornado in Texas?*, 139th meeting of the American Association for the Advancement of Science, 1972, 181.

[381] Majeed M., An Open Letter to Donald Trump by an 18-Year-Old Muslim American Student, Seventeen, 27 Mar. 2015, available at https://www.seventeen.com/life/real-girl-stories/a36525/open-letter-donald-trump-18-year-old-muslim-american-student/.

as a terrorist while living in the US. Within this framework, a few years back, just before the 2016 US Presidential elections, Amara addressed Donald Trump as '*a demagogue'* in an open letter and accused him of *'capitalizing on Americans' fear and paranoia*', legitimising hate-speech and harassment against 1.6 billion of American Muslims.[382] Considering all these intricate elements, the "no harm" of Amara's story makes it a "good luck" one, as it could have turned out more tragically.

The above-mentioned episodes may give the idea of a weak rule of law, where individuals and vulnerable groups may feel overexposed not only to more and more hateful political discourses but also to dubious investigative practices. Such feelings, due to a system that seems to blindly pursue "absolute forms" of *justice* or *security*, have an impact on the trust individuals place in institutions and in the overall system.

In this regard, studies in social sciences suggest that the legitimacy of an authority is "validated" by the perception its subsidiaries have of the decision-making procedures they could be subject to.[383] According to this view – articulated through the concept of 'procedural justice'[384] – social groups assess legal procedures according to *criteria* such as: (1) the neutrality of the decision-maker, (2) the level of dignity received during the procedure, and (3) the possibility to intervene and participate to the processes involving their status.[385]

Evaluations about the 'neutrality' of the authority involve the objectivity/impartiality of a decision-making process. It should be based on facts and pre-determined sets of rules, leaving apart all the biases potentially influencing the final outcome.[386] Having made these points, the 'non-neutrality' of the deployment of FRSs by law enforcement agencies could be argued under a double perspective. On the one hand, current FRSs still show a strong 'technical immaturity' given by significant error

[382] *Ibid.*

[383] Tyler T. R., *Social justice: Outcome and procedure*, International journal of psychology, 35(2), 2000, 117-125, 120; by the same author see also *Procedural justice, legitimacy, and the effective rule of law*, Crime and Justice, 30, 283-357.

[384] Tyler T. R., *What is Procedural Justice?: Criteria used by Citizens to Assess the Fairness of Legal Procedures*, Law & Society Review, (22)1, 1988, 103-136.

[385] *Ibid.*

[386] *Ibid.*

rates and their higher incidence towards certain categories, ethnic and age groups. On the other hand, uses as those mentioned before display disrespect for whatsoever standard of conduct and rule of procedure.

Moving onward, it is not hard to imagine how investigative practices conducted by the use of technological instruments, error-prone, frequently discriminatory in their outcomes, and improperly used, might not only reduce the trustworthiness in the institutions, but also make people feel degraded in their human dignity – *a fortiori* in we consider the strict correlation between this concept and the deployment of FRT already shown.[387]

These considerations also relate to the third said *criterion*. Namely, the possibility to intervene and participate in decision-making processes. Of course, while dealing with criminal matters, particularly during the investigations, the role of the suspect investigated is passive by nature, since the information related to inquisitorial investigations is to a certain extent confidential. Yet, even during the trial, indictments resulting from the use of FRT cannot be contested as it would be for the testimony of an eyewitness. In fact, while testimony could be subject to cross-examination in court, the way of functioning of such algorithms is in the first place obscure and opaque. Also, this *black box effect* would assume a double nature each time it entails not only the operational non-interpretability of algorithmic decision-making processes, but also '*legal black boxes*' screening FRSs as proprietary software subjected to IP and trade-secrecy laws.[388]

[387] On the possibility of individuals to feel '*their value as human being lessened*' when relevant decision-making processes are conferred to computers, see Simmons R., *supra* note 232, 577.

[388] Introna I. *et al.*, *supra* note 121, 183. See also Crawford K., *Regulate facial-recognition technology*, World View, Springer Nature, 572, 2019, particularly for the expression '*legal "black box"*'. On these themes see also Foryciarz A., Leufer D. and Szymielewicz K., *Black-Boxed Politics: Opacity is a Choice in AI Systems*, Panoptycon Foundation, 17 Jan. 2020, available at https://en.panoptykon.org/articles/black-boxed-politics-opacity-choice-ai-systems.

In this way, the blind reliance on FRT identification may also undermine principles as the presumption of innocence by substantially reversing the burden of proof on the accused. In fact, the excessive faith in forms of algorithmics decision-making can degenerate in *automation biases*, thus referring to '*the propensity for humans to assume that automated decision making systems are infallible and to ignore contradictory information made without automation, even if it is correct'.* [389]

Such tendencies overlook that automated processes generally mirror fallacies or biases of their designers.[390] A clear example in this sense is the case of predicting policing algorithms, which are 'designed' to analyse the data they are trained with to extract and 'reproduce' patterns of future criminal activity.[391] Their usage frequently results in *self-fulfilling prophecies*, indeed when the training data concern areas factually more surveilled because historically believed more prone to crime, algorithmic-driven intensified patrolling are bound to produce even future higher and higher rates of crime.[392]

This last analysis shows how irresponsible uses of advanced yet dangerous technologies by law enforcement may undermine the respect for European rule of law standards. This appears to be the case of the prevention of abuse of powers or the respect for several aspects of the right to a fair trial highlighted above.[393]

---

[389] Korff D. & Georges M., *Passenger Name Records, data mining & data protection: the need for strong safeguards*, CoE Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [T-PD(2015)11], Jun. 2015, 29-30.

[390] FRA, *supra* note 17, 27; Dushi D., *supra* note 268, 4.

[391] Hardyns W. & Rummens A., *Predictive policing as a new tool for law enforcement? Recent developments and challenges*, European journal on criminal policy and research, 24(3), 2018, 201-218; Ferguson, A. G., *Policing predictive policing*, Washington University Law Review, 94(5), 2017, 1109-1190; McCarthy O. J., *AI & Global Governance: Turning the Tide on Crime with Predictive Policing*, United Nations University (Centre for Policy Research), published on 26 Feb. 2019, available at https://cpr.unu.edu/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html.

[392] Lum K. & Isaac W., *To predict and serve?*, Significance, 13(5), 2016, 14-19, 16.

[393] Venice Commission, *The Rule of Law Checklist*, Council of Europe, 2016; respectively 29 *et seq*, 42 *et seq.*

3. *The rule of law as a prerequisite for human rights and social justice. Conclusions.*

This chapter gave the chance to explore the world of FRT from a slightly different angle. The episodes presented and the theoretical background here adopted seem to unveil that the issues and doubts raised by current uses of FRT in law enforcement go far beyond the several fictions related to fundamental rights and freedoms already analysed. In a view which sees the mutual interrelation among human rights and the rule of law, the respect for its standards is a prerequisite for an effective protection of fundamental rights and freedoms.[394] In this respect, it has emerged that public servants increasingly resort to unreliable instruments intensifying the risks of FRT with their questionably lawful conducts, instead of overcoming technological shortcomings with professionalism and rigid standards.

This results in serious implications with regard to core principles of the rule of law as accountability, inclusion, participation, and transparency.[395] Such repercussions may exacerbate several weaknesses seriously affecting our societies *i.a.* in terms of equality, social justice, gender or racial-based discrimination.[396] Whilst the deployment of various forms of FRT by law enforcement should pursue enhanced levels of security within our communities, in light of the above, such systems should be strongly opposed by the general public and entrusted of a very poor social legitimisation, as the risks connected to their deployment seems to be way more than the correspondingly attainable benefits.

---

[394] *Ibid.*, 11.

[395] van Hout B., Regional Representative for Europe of the Office of the UN High Commissioner for Human Rights (OHCHR), in *The Case for a Human Rights Approach to the Rule of Law in the European Union*, Publication of the United Nations Human Rights Regional Office for Europe, May 2020, iii; Venice Commission, *supra* note 394.

[396] Naranjo D., *Your face rings a bell. How facial recognition poses a threat for human rights*, Global Campus of Human Rights (Europe) Policy Briefs, 2020, 10.

Conclusions

Despite the wide range of issues related to FRT use by law enforcement shown by the present research, nothing seems to stop its rapid expansion. Although several authorities at both the European and international level have raised various concerns on the matter,[397] any specific regulation of FRSs has been adopted yet. In this regard, the current approaches range from those advocating for a ban of FRT by the EU,[398] to those suggesting strict regulations for specific purposes – as, for instance, those related to law enforcement activities.[399] Yet, in a context dominated by forms of '*technological determinism*'[400] and '*infrastructure imperialism*'[401], the pace would seem to be set by the private companies that produce those systems (*e.g.*, Clearview AI). Within this complex scenario, there are also private actors taking a stand on contemporary issues of great social importance. Recently, IBM, Microsoft, and Amazon have publicly voiced against the use of FRT as an instrument of mass surveillance that may impact on fundamental rights and freedoms.[402]

In the meanwhile, the tangible results of the steady process of normalisation of surveillance, stemming from the abuse of security discourses as a statutory backdoor

---

[397] *i.a.* Wiewiórowski W., *Facial recognition: A solution in search of a problem?*, European Data Protection Supervisor (EDPS), 28 Oct. 2019, available at https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en; from the same author, *AI and Facial Recognition: Challenges and Opportunities*, EDPS, published on 21 Feb. 2020, available at https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en. Mijatović D., *Safeguarding human rights in the era of artificial intelligence*, Commissioner for Human rights CoE, 3 Jul. 2018, available at https://www.coe.int/en/web/commissioner/-/safeguarding-human-rights-in-the-era-of-artificial-intelligence. *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, Annual report of the United Nations High Commissioner for Human Rights, 24 June 2020, UN Doc. A/HRC/44/24.

[398] Jakubowska E. *et al.*, *supra* note 93; Naranjo D., *supra* note 397.

[399] Dushi D., *supra* note 268.

[400] Kranzberg M., *supra* note 73, 545.

[401] Zuboff S., *supra* note 10, 78, 79, and the literature therein mentioned.

[402] Magrid L., IBM, Microsoft and Amazon not letting Police use Facial Recognition Technology, Forbes, 12 Jun. 2020, available at https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/.

for indulgence towards surveillance measures, should trigger the alarm bell. Although technological means appear as "soft forms" of surveillance if compared to more evidently intrusive models of social control, they are not to be considered less dangerous.[403] Once the path towards a devaluation of fundamental rights and freedoms in the name of "higher values" of security has been taken, reversing the trend back may equate to fighting a losing battle. If action is not taken in due time, the dangers of a looming future can already be imagined looking East. If the aforementioned examples about the growing Russian surveillance infrastructure are not concerning enough,[404] perhaps, the Chinese ubiquitous use of facial recognition would be so. There, since December 2019, the registration of facial biometrics is a mandatory requirement to access communication and mobile data services.[405] Yet, the use of such biometric data made by the Chinese government is not heartening, as it encompasses the targeting of the Uighur Muslim minority and the dystopian 'social credit' system, which assigns scores to the citizens also based on their behaviours in public spaces and interactions with other citizens,[406] as in the case of real-time 'name and shame' campaigns against

[403] '*The "softness" of surveillance measures contributes to their legal receptiveness and apparently silences civil liberty arguments.*', see De Hert P., *Post-September 11 changes in the public discourse and policy making on security*, Utrecht Law Review (1), 2005, 68-96, 90. This argument is made on the '*non-intrusive, contact-free process*' of this kind of measures; the quoted characteristics in their original context were labelled as one of the '*[a]dvantages of Facial Recognition Surveillance*' in Woodward J. D., Horn C., Gatune J, and Thomas A., *Biometrics, A Look at Facial Recognition*, Documented briefing prepared for the Virginia State Crime Commission, Rand Public Safety and Justice, 2003, 7.

[404] Habersetzer N., *supra* note 7; see also *supra* Chapter II., *Section 5.4*.

[405] *China due to introduce face scans for mobile users*, BBC NEWS, Dec. 1, 2019, available at https://www.bbc.com/news/world-asia-china-50587098.

[406] *Ibid.* See also Kaye D., *supra* note 204; Wang M., *The Robots are Watching Us*, Human Rights Watch, April 6, 2020, available at https://www.hrw.org/news/2020/04/06/robots-are-watching-us; *Big Brother is watching: how China is compiling computer rating on all its citizens*, South China Morning Post, 24 Nov. 2015, available at https://www.scmp.com/news/china/policies-politics/article/1882533/big-brother-watching-how-china-compiling-computer; Jing Zeng M., *China's Social Credit System puts its people under pressure to be model citizens*, The Conversation, 23 Jan. 2018, available at https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963.

traffic offenders.[407] In this regard, some claim that '*what occurs in China will re-occur in western democracies within five to ten years*'.[408] Hence, what can be done before it is too late?

The present research appears to have gathered sufficient arguments to hold that, currently, there is no 'pressing social need' that would justify uses of FRT so disruptive for fundamental rights and democratic values as those analysed throughout this paper. Conversely, there is certainly an urgent need for regulation and, until the deployment of such technologies is not adequately governed, a ban of their use sounds as a reasonable "solution". As long as there is a lack of a firm stand about FRSs use by the EU, foreign companies will continue to develop and offer their products to European actors, making it harder to *ex post* dismantle the infrastructures meanwhile put into place. Finally, the same attitude will not discourage the outrageous and unlawful use of European citizens' data, as occurring in the case of Clearview AI. On the contrary, public authorities' interest in these instruments might be a pull factor, encouraging dubious companies to develop powerful tools that pose a serious threat to fundamental rights.

Yet, there is something odd. Not always the threat comes from afar. In fact, it seems that, through the Horizon 2020 funding scheme, the European Commission has significantly invested in R&D in the fields AI-based surveillance technologies.[409]

Therefore, waiting for EU taking up a clear position on this topic, the sole reliance on top-down regulatory initiatives may not suffice.

Several times during this composition the "pathological" human dependence on technology has been emphasised. In this view, a primary objective to be achieved for the protection of our rights is to raise public awareness about the importance of the respect for private spheres, as the enabling environment for human flourishing. On it,

---

[407] Yu K., *Facial recognition: Concerns over China's widespread surveillance*, Aljazeera, 18 Feb. 2020, available at https://www.aljazeera.com/news/2020/02/facial-recognition-concerns-chinas-widespread-surveillance-200218111532668.html.
[408] Crampton J. W., *supra* note 212, 61.
[409] Privacy International, *MONITORYOU: the MilliONs being spent by the eu on developing surveillance tech to target YOU*, available at https://privacyinternational.org/long-read/3341/monitoryou-millions-being-spent-eu-developing-surveillance-tech-target-you.

depends the variability of individual personalities, which fuel the functioning of healthy pluralist societies.

If a radical change of direction is not undertaken soon, forms of resistance constitute all that is left. For example, while the rapid spread of FRSs takes place in Belgrade, spontaneous citizens' initiatives rise. This is the case of *hijiade.kamera.rs* (Thousands of Cameras), a website providing information about the governmental use of surveillance technologies; in the lack of transparency and information to the public, about the deployment of FRT in public spaces,[410] the citizens spontaneously point out and map online the cameras spotted around the city, asking for more transparency and accountability.[411] Also, several researchers and manufacturers have started working on face masks and "fashion accessories" designed to "confuse" FRSs and avoid the detection of our faces.[412] If in the future such equipment will be the only way to preserve anonymity in public spaces, many of us would probably be well-trained, after being used to wear face masks for months due to the COVID-19 pandemic. Yet, in that case, one might wonder what happened to the concept of 'human dignity' if the only way to protect our anonymity would be to constantly disguise our distinctive facial traits. And, if at that point the possibility to wear face masks in public spaces would also be banned – as contemplated to curb the 2019-2020 Honk Hong protests, one would be curious to see – continuing the pandemic – who will win in the clash of the titans between the pursuit of public security and the protection of public health.

---

[410] *New surveillance cameras in Belgrade: location and human rights impact analysis – "withheld"*, Share Foundation, 19 Mar. 2019, available at https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/.

[411] *hiljade.kamera.rs: community strikes back against mass surveillance*, Share Foundation, 19 May 2020, available at https://www.sharefoundation.info/en/hiljade-kamera-rs-community-strikes-back/.

[412] Holmes A., These clothes use outlandish designs to trick facial recognition software into thinking you're not human, Business Insider, 5 Jun. 2020, available at https://www.businessinsider.com/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10?IR=T.

BIBLIOGRAPHY

Books and Articles

Aalto P., Hofmann H. C., Holopainen L., Paunio E., Pech L., Sayers D., Shelton D. & Ward A., *Right to an effective remedy and to a fair trial*, in *The EU Charter of Fundamental Rights: A Commentary*. Ed. Peers S., Hervey T., Kenner J. and Ward A., Hart Publishing, 2014, 1197-1276;

Agre P.E., *Surveillance and capture: Two models of privacy*, The information society, 10(2), 1994, 101-127; see also Pell S. K., *Location Tracking*, in Gray D. & Henderson S. E. (Eds.), *The Cambridge Handbook of Surveillance Law*. Cambridge University Press 2017, 44-70;

Andalibi N. & Buss J., *The Human in Emotion Recognition on Social Media: Attitudes, Outcomes, Risks*, Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, 1-16.

Aolain F., *How can states counter terrorism while protecting human rights*, Ohio Northern University Law Review, 45(2), 2019, 389-410;

Baldwin D. A., *The concept of security*, in Review of International Studies, 23(1), 1997, 5-26;

Barak A., *A Judge on Judging: The Role of a Supreme Court in a Democracy*, Harvard Law Review, 116(1), 2002, 19-162;

Barkhuysen T., van Emmerik M., Jansen O. & Fedorova M., *Right to a fair trial*, in Van Dijk P., Van Hoof F., Van Rijn A., Zwaak L. (Eds), *Theory and Practice of the European Convention on Human Rights*, 5th Ed., Intersentia, 2018, 497-654;

Barnard-Wills D., & Wells H., *Surveillance, technology and the everyday*, in Criminology & Criminal Justice, 12(3), 2012, 227-237;

Barrett L. F., Adolphs R., Marsella S., Martinez A. M., & Pollak S. D., *Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements*, Psychological Science in the Public Interest, 20, 1–68;

Bauman Z., Bigo D., Esteves P., Guild E., Jabri V., Lyon D. & Walker R. B., A*fter Snowden: Rethinking the impact of surveillance* in International political sociology, 8(2), 2014, 121-144;

Broeksteeg H., *Freedom of Assembly and Association*, in Van Dijk P., Van Hoof F., Van Rijn A., Zwaak L. (Eds), *Theory and Practice of the European Convention on Human Rights*, 5th Ed., Intersentia, 2018, 813-835;

Büchi M., Fosch-Villaronga E., Lutz C., Tamò-Larrieux A., Velidi S. & Viljoen S., *The chilling effects of algorithmic profiling: Mapping the issues*, Computer Law & Security Review, 2020;

Bygrave, L. A., *Data privacy law: an international perspective*, Oxford University Press, 2014;

Calo, R., *Artificial intelligence policy: primer and roadmap*, U.C. Davis Law Review, 51(2), 2017, 399-436;

Caruana, M. M., *The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement*, International Review of Law, Computers & Technology, 33(3), 2019, 249-270;

Casagran C. R., *Surveillance in the European Union*, in Gray D., & Henderson S. E. (Eds.), *The Cambridge Handbook of Surveillance Law*. Cambridge University Press 2017, 643-658;

Chesney B. & Citron D., *Deep fakes: A looming challenge for privacy, democracy, and national security*, Calif. L. Rev., 107, 2019, 1753-1820;

Chesney R. & Citron D., *Deepfakes and the new disinformation war: The coming age of post-truth geopolitics*, Foreign Affairs, 98(1), 147-155;

Clarke R., *Information technology and dataveillance*, Communications of the ACM, 31(5), 1988, 498-512;

Crampton J. W., *Platform biometrics*, Surveillance & Society, 17(1/2), 2019, 54-62;

De Hert P., *Post-September 11 changes in the public discourse and policy making on security*, Utrecht Law Review (1), 2005, 68-96;

De Vries K., *Right to Respect for Private and Family Life*, in Van Dijk P., Van Hoof F., Van Rijn A., Zwaak L. (Eds), *Theory and Practice of the European Convention on Human Rights*, 5th Ed., Intersentia, 2018, 667-734;

Dignum V., *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*, Springer International Publishing, 2019;

Dupré C., *Human Dignity*, in *The EU Charter of Fundamental Rights: A Commentary*. Ed. Peers S., Hervey T., Kenner J. and Ward A., Hart Publishing, 2014, 4-24;

Dushi D., *The use of facial recognition technology in EU law enforcement: Fundamental rights implications*, Global Campus (South East Europe) Policy Briefs 2020;

Ekman P., *Universal Facial Expressions of Emotion*, California Mental Health Research Digest, 8(4), 1970, 151-158;

Ekman P. & Friesen W. V., *Unmasking the face: A guide to recognizing emotions from facial clues*, Prentice-Hall, 1975;

Ekman P., Sorenson E. R. & Friesen W. V., *Pan-cultural elements in facial displays of emotion*, Science, 164(3875), 1969, 86-88;

Elish M. C. & Boyd D., *Situating methods in the magic of Big Data and AI*, Communication monographs, 85(1), 2018, 57-80;

Ferguson A. G., *Big Data Surveillance: The Convergence of Big Data and Law Enforcement*, in Gray D. & Henderson S. E. (Eds.), *The Cambridge Handbook of Surveillance Law*. Cambridge University Press 2017, 171-197;

Floridi L. & Sanders J. W., *On the morality of artificial agents*, Minds and machines, 14(3), 2004, 349-379;

Friedland S. I., *The Internet of Things and Self- Surveillance Systems*, in Gray D., & Henderson S. E. (Eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge University Press 2017, 199-223;

Gearty C., *Terrorism and human rights*, Government and Opposition, 42(3), 2007, 340-362;

Gerards J., *Relationship between the Convention and the EU*, in Van Dijk P., Van Hoof F., Van Rijn A., Zwaak L. (Eds), *Theory and Practice of the European Convention on Human Rights*, 5th Ed., Intersentia, 2018, 331-352;

Girasa, R., *Artificial Intelligence as a Disruptive Technology*, Palgrave Macmillan, 2020;

Goold B. J., *Trusted Travellers and Trojan Horses: Security, Privacy, and Privilege at the Border*, in Goold B. J. & Lazarus L. (Eds.), *Security and human rights*, Bloomsbury Publishing, 2019, 125-144;

Goold B. J. & Lazarus L. (Eds.), *Security and Human Rights*, Bloomsbury Publishing, 2019;

Gragl P., *Agreement on the Accession of the European Union to the European Convention on Human Rights*, in *The EU Charter of Fundamental Rights: A Commentary*. Ed. Peers S., Hervey T., Kenner J. and Ward A., Hart Publishing, 2014, 1727-1824;

Gray D. & Henderson S. E. (Eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge University Press, 2017;

Greene A., *Permanent States of Emergency and the Rule of Law: Constitutions in an Age of Crisis*. Bloomsbury Publishing, 2018;

Haggerty K. D., Wilson D. &. Smith G. J, in *Theorizing surveillance in crime control,* Theoretical criminology, 15(3), 2011, 231-237;

Introna L. & Wood D., *Picturing algorithmic surveillance: The politics of facial recognition systems*, Surveillance & Society, 2(2/3), 177-198;

Jean N., Burke M., Xie M., Davis W. M., Lobell D. B. & Ermon S., *Combining satellite imagery and machine learning to predict poverty*, Science (80-.)353, 2016, 790-794;

Jiang R., Al-Maadeed S., Bouridane A., Crookes, D., & Beghdadi, A., *Biometric Security and Privacy*, Springer International Publishing, 2017;

Joergensen R. F., *Can human rights law bend mass surveillance?*, Internet Policy Review 3(1), 2014, 1-9;

Kemp L. *et al*., *UN High-level Panel on Digital Cooperation: A Proposal for International AI Governance*, 2019, available at https://digitalcooperation.org/wp-content/uploads/2019/02/Luke_Kemp_Submission-to-the-UN-High-Level-Panel-on-Digital-Cooperation-2019-Kemp-et-al.pdf;

Kranenborg H., *Protection of personal data*, in *The EU Charter of Fundamental Rights: A Commentary*. Ed. Peers S., Hervey T., Kenner J. and Ward A., Hart Publishing, 2014, 223-265;

Kranzberg M., *Technology and History:" Kranzberg's Laws"*, Technology and culture, 27(3), 1986, 544-560;

Kumm M., *The cosmopolitan turn in constitutionalism: an integrated conception of public law*, Indiana J Global Legal Studies 2013;

Land M. K. & Aronson J. D., *The Promise and Peril of Human Rights Technology*, in New Technologies for Human Rights Law and Practice, Cambridge University Press, 2018, 1-20;

Latonero M., *Governing artificial intelligence: Upholding human rights & dignity*, Data & Society, 2018;

Lavrysen, L., *System of Restrictions*, in Van Dijk P., Van Hoof F., Van Rijn A., Zwaak L. (Eds), *Theory and Practice of the European Convention on Human Rights*, 5th Ed., Intersentia, 2018, 307-330;

Leiser, M. R., & Custers, B. H. M., *The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680*, European Data Protection Law Review, 5, 12, 2019;

Levinson-Waldman R., *NSA Surveillance in the War on Terror*, in Gray D., & Henderson S. E. (Eds.), *The Cambridge Handbook of Surveillance Law*. Cambridge University Press 2017, 7-43;

Lippens R. & Gardiner-Bess R., *Technologies of crime control: international developments and contexts*, in Arrigo B., & Bersot H. (Eds.), *The Routledge handbook of international crime and justice studies*, Routledge, 2013, 350-370;

Lombroso, C., L'uomo delinquente (1876). *Hoepli*, 1971;

Lyon D., *Surveillance Society,* Talk for Festival del Diritto, Piacenza, Italia, 2008;

Malgieri, G., & De Hert, P., *European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably But Not Necessarily by Judges*, in Gray D. & Henderson S. E. (Eds.), *The Cambridge Handbook of Surveillance Law*, Cambridge University Press, 2017, 509-532;

Manheim K. & Kaplan L., *Artificial Intelligence: Risks to Privacy and Democracy*, Yale Journal of Law & Technology, 21(1), 2019, 106-189;

Mayer-Schönberger V. & Cukier K., *Big data: A revolution that will transform how we live, work. In and Think*, John Murray Publishers Ltd London, 2013;

Marcella A. J. & Stucki C., *Privacy Handbook: Guidelines, Exposures, Policy Implementation and International Issues*, Hoboken, NJ: John Wiley & Sons, 2003, XIX;

Marx, G. T., *What's New About the "New Surveillance"? Classifying for Change and Continuity*, Surveillance & Society, 1(1), 2002, 9-29;

McCarthy J., *What Is AI? / Basic Questions*, in Jmc.Stanford.Edu. 2018, available at http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html;

McCarthy J., Minsky M. L., Rochester N. & Shannon C. E., *A proposal for the Dartmouth summer research project on artificial intelligence*, 1955, in AI magazine, 27(4), 2006, 12;

Miller K., *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, Journal of Technology Law & Policy 19(1), 2014, 105-146;

Minsky M., *The Emotion Machine*, Simon and Schuster, 2006;

Minsky M., *The Society of Mind*, Simon and Schuster, 1988;

Mordini E., *Ethics and Policy of Biometrics*, in Tistarelli M., Li S. Z. and Chellappa R. (Eds), *Handbook of Remote Biometrics for Surveillance and Security*, Springer, 2009, 293-312;

Nemitz P., *Constitutional democracy and technology in the age of artificial intelligence*, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2018;

Pantserev K.A., *The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability*, in Jahankhani H., Kendzierskyj S., Chelvachandran N., Ibarra J. (Eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Springer, 2020, 37-55;

Pavone V., Santiago Gomez E., & Jaquet-Chifelle D. O., *A systemic approach to security: beyond the tradeoff between security and liberty*, in Democracy and Security, 12(4), 2016, 225-246;

Peers S., Hervey T., Kenner J. and Ward A., *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2014;

Peers S. and Prechal S., *Scope and Interpretation of Rights and Principles*, in *The EU Charter of Fundamental Rights*, *The EU Charter of Fundamental Rights: A Commentary*, Hart Publishing, 2014, 1455–1522;

Piza E. L., Welsh B. C., Farrington D. P. & Thomas A. L., *CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis*, Criminology & Public Policy, 18(1), 135-159;

Raso F. A., Hilligoss H., Krishnamurthy V., Bavitz C. & Kim L., *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center Research Publication, (2018-6), 2018;

Richards N. M., *The dangers of surveillance*, Harv. L. Rev., 126, 2012, 1934

Rosas A., *The Charter and Universal Human Rights Instruments*, in *The EU Charter of Fundamental Rights: A Commentary*, Ed. Peers S., Hervey T., Kenner J. and Ward A., Hart Publishing, 2014;, 1685-1702;

Rothschild E., *"What Is Security?"*, Daedalus 124(3), 1995, 53-98;

Samuel A. L., *Some Moral and Technical Consequences of Automation – A Refutation*, Science 132(3429), 1960, 741-742;

Sarre R., Brooks D., Smith C. & Draper R., *Current and emerging technologies employed to abate crime and to promote security*, in Arrigo B. &

Bersot H. (Eds.), *The Routledge handbook of international crime and justice studies*, Routledge, 2013, 327- 349;

Scott, P. F., *The National Security Constitution*. Bloomsbury Publishing, 2018;

Simmons R., *Big data and procedural justice: Legitimizing algorithms in the criminal justice system*, Ohio State Journal of Criminal Law, 15(2), 2018, 573-582;

Skogan W. G., *The future of CCTV*, Criminology & Public Policy, 18(1), 2019, 161-166;

Smith C., McGuire B., Huang T. & Yang G., *The history of artificial intelligence*, University of Washington, 2006;

Stark L., *Facial recognition is the plutonium of AI*, XRDS: Crossroads, The ACM Magazine for Students, 25(3), 50-55;

Stoycheff E., Liu J., Xu K., & Wibowo K, *Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects*, New media & society, 21(3), 602-619;

Sulowski S., *Counter-Terrorism: Correlating Security and Freedom*, in Sroka A., Castro-Rial Garrone F., and Torres Kumbrián R. D. *Radicalism and Terrorism in the 21st Century*, Peter Lang AG, 2017, 11-23;

Taddeo M. & Floridi L., *How AI can be a force for good*, Science, 361(6404), 2018, 751-752;

Tecuci G., *Artificial Intelligence*, WIREs Comput Stat, 4/2012, 2012, 168-180;

Van der Sloot B., *Privacy as human flourishing: could a shift towards virtue ethics strengthen privacy protection in the age of Big Data*, J. Intell. Prop. Info. Tech. & Elec. Com. L., 5, 2014, 230-244;

Van Dijk P., Van Hoof F., Van Rijn A., Zwaak L. (Eds), *Theory and Practice of the European Convention on Human Rights*, 5th Ed., Intersentia, 2018;

Vervaele, J. A., *Surveillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system?*, In Reloading Data Protection, Springer, 2014, 115-128;

Vinuesa R., Azizpour H., Leite I., *et al.*, *The role of artificial intelligence in achieving the Sustainable Development Goals*, Nature Communications 11, 2020;

Wang Y. & Kosinski M., *Deep neural networks are more accurate than humans at detecting sexual orientation from facial images*, Journal of personality and social psychology, 114(2), 2018, 246;

Wilson D. & McCulloch J., *Pre-crime: Pre-emption, precaution and the future*, Routledge, 2017;

Wolfers A., *"National security" as an ambiguous symbol*, Political science quarterly, 67(4), 1952, 481-502;

Wu X. & Zhang X., *Automated Inference on Criminality using Face Images*, *arXiv preprint arXiv:1611.04135*, 2016, 4038-4052;

Zahid M., Nazeer M., Nargis B., Tauseef A., *A Review on state-of-the-art face recognition approaches*, Fractals, 25(2) 2017;

Zedner L., *Pre-crime and post-criminology?*, Theoretical criminology, 11(2), 2007, 261-281;

Zuboff S., *Big other: surveillance capitalism and the prospects of an information civilization*, Journal of Information Technology, 30(1), 2015, 75-89;

Zuboff S., *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books, 2019.

Official Documents and Reports

Access now, *Human rights in the age of artificial intelligence*, 2018;

AI Now, *Report 2018, 2018*;

AI Now, *Report 2019, 2019*;

Amnesty International & Access Now, *The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems.*, 2018, available at https://www.torontodeclaration.org/declaration-text/english/;

Azria S. and Wickert F., *Facial Recognition: Current Situation and Challenges*, Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data [T-PD(2019)05rev], 2019;

Besaw C. & Filitz J., *Artificial Intelligence in Africa is a Double-edged Sword*, United Nations University (Centre for Policy Research), published on Jan. 16th 2019, available at https://ourworld.unu.edu/en/ai-in-africa-is-a-double-edged-sword;

Brundage M. *et al*., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, Technical Report, 2018;

Chinese police spot suspects with surveillance sunglasses, BBC NEWS, published on 7th Feb. 2018, available at https://www.bbc.com/news/world-asia-china-42973456;

Communication from the Commission to the European Parliament and the Council, *A new EU Framework to strengthen the Rule of Law*, 11 Mar. 2014, COM(2014) 158 final;

Communication from the Commission to the European Parliament, the European Council, the Council, the European economic and social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, 24 Apr. 2018, COM(2018) 237 final;

Council of Europe, PACE Committee on Legal Affairs and Human Rights, Report on Mass Surveillance, AS/Jur (2015) 01;

Council of Europe, PACE Recommendation, *Technological convergence, artificial intelligence and human rights*, 28 Apr. 2017, 2102(2017);

Council of Europe, PACE Resolution 21st Apr. 2015, 2045(2015);

Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192*, adopted on 22nd Mar. 2012;

Davies B., Innes M. and Dawson A., *An evaluation of South Wales police's use of Automated Facial Recognition*, Universities' Police Science Institute Crime & Security Research Institute, Cardiff University, 2018;

Docherty B. L., *Shaking the foundations: The human rights implications of killer robots*, Human Rights Watch, 2014;

European Commission, *White paper on Artificial Intelligence – A European approach to excellence and trust*, 19 Feb. 2020, COM(2020)65 final;

European Commission for the Effectiveness of Justice (CEPEJ), *European ethical Charter on the use of Artificial Intelligence in Judicial Systems and their environment*, Council of Europe, 2018;

European Data Protection Board (EDPB), *Guidelines 3/2019 on processing of personal data through video devices*, 2019;

European Data Protection Board (EDPB), *Response to MEPs concerning the facial recognition app developed by Clearview AI*, published on 10th Jun. 2020, available at

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf;

European Data Protection Supervisor (EDPS), *Assessing the necessity of measures that limit the fundamental rights to the protection of personal data: A Toolkit*, 2017;

European Parliament LIBE and JHA Committee Report, 21st Feb. 2014 [A7-0139/2014];

European Parliament, Resolution 12 Mar. 2014, (2013/2188(INI) [P7_TA(2014)0230];

European Parliament, Resolution 29 Oct. 2015 [P8_TA(2015)0388];

European Union Agency for Fundamental Rights (FRA), *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019;

European Union Agency for Fundamental Rights (FRA), *Preventing unlawful profiling today and in the future: a guide*, 2018;

European Union Agency for Fundamental Rights (FRA), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, 2018;

European Union Agency for Fundamental Rights (FRA) and Council of Europe (CoE), *Handbook on European data protection law*, 2018 Edition, 2019;

Freedom House, *China Country Report*, 2020, available at https://freedomhouse.org/country/china/freedom-world/2020;

Fussey P., & Murray D., *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology,* The Human Rights, Big Data and Technology Project, University of Essex, 2019;

Future of Life Institute, *Autonomous weapons: An open letter from AI & robotics researchers*, 2015, available at https://futureoflife.org/open-letter-autonomous-weapons/;

Garvie C., Bedoya A. M., Frankle J., *The Perpetual Line-Up – Unregulated Police Face Recognition in America*, Georgetown Law University, Center on Privacy & Technology, 2016;

Guterres A., *UN Secretary-General's Strategy on New Technologies*, United Nations, September, 2018 available at https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf;

Hardoon D., *An economy for the 99%*, Oxfam Policy Papers, 2017;

Heyns C., *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions*, United Nations Doc. A/HRC/23/47, 2013;

High-Level Expert Group on Artificial Intelligence established by the European Commission, *A definition of AI: Main Capabilities and Disciplines*, published on 8th Apr. 2019;

*How AI Can Improve Agriculture for Better Food Security***,** AI for Good - Global Summit 28th-31st May 2019, International Telecommunication Union (ITU-UN), available at https://itu.foleon.com/itu/aiforgood2019/ai-and-agriculture/;

Information Commissioner's Office & The Alan Turing Institute, *Explaining decisions made with AI, Part: 2*, 2019;

INTERPOL dedicated page available at https://www.interpol.int/Crimes/Terrorism/Identifying-terrorist-suspects;

INTERPOL dedicated page available at https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition;

Introna L. & Nissenbaum H., *Facial recognition technology a survey of policy and implementation issues*, Working Paper 2010/030, Lancaster University Management School, 2010;

Jakubowska E. & Naranjo D., *Ban Biometric Mass Surveillance A set of fundamental rights demands for the European Commission and EU Member States*, EDRi, - European Digital Rights, published on 13th May 2020, available at https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf;

Jing Zeng M., *China's Social Credit System puts its people under pressure to be model citizens*, The Conversation, published on 23rd Jan. 2018, available at https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963;

Kaye D., *Surveillance and Human Rights*, UN Doc. A/HRC/41/35, 2019;

Kornfeld-Matte R., *Report of the Independent Expert on the enjoyment of all human rights by older persons*, United Nations Doc. A/HRC/36/48, 2017;

Kramer A. D., Guillory J. E., & Hancock J. T., *Experimental evidence of massive-scale emotional contagion through social networks*, Proceedings of the National Academy of Sciences, 111(24), 2014, 8788-8790;

La Rue F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UN Doc. A/HRC/23/40, 2013;

Legrain P. and Lee-Makiyama H., *Ever Clever Union How AI could help EU institutions become more capable, competent, cost-effective and closer to citizens*, Open, 2019;

Levin S., *Face-reading AI will be able to detect your politics and IQ, professor says*, The Guardian, published on 12th Sep. 2017, available at https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski;

Li P. & Cadell C., *China eyes 'black tech' to boost security as parliament meets*, Reuters, published on 10th Mar. 2018, available at https://www.reuters.com/article/us-china-parliament-surveillance/china-eyes-black-tech-to-boost-security-as-parliament-meets;

Lynch J., *Face Off Law Enforcement use of facial recognition technology*, Electronic Frontier Foundation (EFF), 2020;

Mijatović D., *Safeguarding human rights in the era of artificial intelligence*, Commissioner for Human rights CoE, 3 Jul. 2018, available at https://www.coe.int/en/web/commissioner/-/safeguarding-human-rights-in-the-era-of-artificial-intelligence;

OHCHR, *CCPR General Comment No. 16: Article 17-The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, Adopted at the 32nd Session of the Human Rights Committee, on 8th April 1988;

OHCHR *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, Annual report of the United Nations High Commissioner for Human Rights, 24 June 2020, UN Doc. A/HRC/44/24;

OHCHR, Report, *The right to privacy in the digital age*, United Nations Doc. A/HRC/27/37, 2014;

Perry W. L., McInnis B., Price C., Smith S. C., and Hollywood J. S., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, RAND Corporation, 2013;

Polonski V., *How artificial intelligence silently took over democracy*, World Economic Forum, published on 9th Aug. 2017, available at https://www.weforum.org/agenda/2017/08/artificial-intelligence-can-save-democracy-unless-it-destroys-it-first;

Polyakova A. & Boyer S. P., *The future of political warfare: Russia, the West, and the coming age of global digital competition*, Brookings Robert Bosch Foundation - Transatlantic Initiative, 2018;

Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, Nlets – the International Justice and Public Safety Network, 2011;

Raaijmakers S., *Artificial Intelligence for Law Enforcement: Challenges and Opportunities*, IEEE Security & Privacy, 17(5), 74-77, 2019;

Report from the Commission to the European Parliament and the Council, *Saving Lives: Boosting Car Safety in the* EU, 12 Dec. 2016, COM(2016)787 final;

Res. *Human Rights, democracy and the rule of law*, United Nations Doc. A/HRC/RES/28/14, 2015;

Royal Society A: Mathematical, Physical and Engineering Sciences, 2018;

Royal Society Working Group (GB), *Machine learning: the power and promise of computers that learn by example*, Technical report, 2017;

Trudy J., *Governing Artificial Intelligence to benefit the UN Sustainable Development Goals*, Sustainable Development, 2020;

UN Human Rights Committee, General comment No. 37 'Article 21', UN Doc. CCPR/C/GC/37, July 27, 2020;

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

United Nations Activities on Artificial Intelligence (AI), International Telecommunication Union (ITU UN), 2019;

United Nations Security Council, Resolution S/RES/2322, 2016;

Université de Montréal, *Montréal Declaration for a Responsible Development of Artificial Intelligence*, 2018, available at https://5dcfa4bd-f73a-4de5-94d8-c010ee777609.filesusr.com/ugd/ebc3a3_5c89e007e0de440097cef36dcd69c7b0.pdf;

US House Committee on Oversight and Reform, Hearing '*Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties*', 2154 Rayburn House Office Building, Washington, DC, 22nd May 2019, available at https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and;

van Est R., Gerritsen J. B. A. & Kool L., *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality*, Expert report for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE), Rathenau Institute, 2017;

Venice Commission, *Opinion on video surveillance in public places by public authorities and the protection of human rights* [CDL-AD(2007)014], 2007;

Venice Commission and ODIHR, *Guidelines on freedom of peaceful assembly (3rd Edition)*, Strasbourg/Warsaw, [CDL-AD(2019)017], 2019;

Villani C., *For a Meaningful Artificial Intelligence towards a French and European Strategy*, 2018, available at https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf;

World Justice Project, *Rule of Law Index 2020*, 2020, available at https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index-2020;

Wagner B., *Algorithms and Human Rights, study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, Committee of experts on internet intermediaries (MSI-NET), 2016;

Wiewiórowski W., *AI and Facial Recognition: Challenges and Opportunities*, EDPS, published on 21 Feb. 2020, available at https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en;

Wiewiórowski W., *Facial recognition: A solution in search of a problem?*, European Data Protection Supervisor (EDPS), published on 28 Oct. 2019, available at https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en;

Winston P.H., *Self-Aware Problem Solving*, Computational models of Human Intelligence Community, Report Number 2, 2018;

Woodward J. D., Horn C., Gatune J, and Thomas A., *Biometrics, A Look at Facial Recognition*, Documented briefing prepared for the Virginia State Crime Commission, Rand Public Safety and Justice, 2003;

Woolley S. C., & Howard P., *Computational propaganda worldwide: Executive summary*, Computational Propaganda Research Project, Working Paper No. 2017.11, Oxford University, 2017.

News and Other Sources

Acker A., *Tracking Disinformation by Reading Metadata*, Medium, published on 17th Jul. 2018, available at https://medium.com/@MediaManipulation/tracking-disinformation-by-reading-metadata-320ece1ae79b;

Ackerman S., *TSA screening program risks racial profiling amid shaky science – study*, The Guardian, published on 8th Feb. 2017, available at https://www.theguardian.com/us-news/2017/feb/08/tsa-screening-racial-religious-profiling-aclu-study;

'At first blush, you look happy-or sad, or angry', Ohio State News, published on 19th Mar. 2018, available at https://news.osu.edu/at-first-blush-you-look-happy--or-sad-or-angry/;

Bannister K., *Understanding Sentiment Analysis: What It Is & Why It's Used*, published in 26th Feb. 2018, available at https://www.brandwatch.com/blog/understanding-sentiment-analysis;

Benitez-Quiroz C. F., Srinivasan R. & Martinez, A. M., *Facial color is an efficient mechanism to visually transmit emotion*, Proceedings of the National Academy of Sciences, 115(14), 3581-358, 2018;

Big Brother is watching: how China is compiling computer rating on all its citizens, South China Morning Post, published on 24th Nov. 2015, available at https://www.scmp.com/news/china/policies-politics/article/1882533/big-brother-watching-how-china-compiling-computer;

Bischoff P., *Surveillance camera statistics: which cities have the most CCTV cameras?*, Comparitech, published on 15th Aug. 2019, available at https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/;

Bonifacic I., *Google tells facial recognition startup Clearview AI to stop scraping photos*, engadget, published on 5th Feb. 2020, available at https://www.engadget.com/2020-02-05-google-tells-clearview-at-stop-scraping-photos.html;

Brandom R., *Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors*, The Verge, published on 11th Oct. 2016, available at https://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api;

Brewster T., *Remember Find Face? The Russian Facial Recognition Company Just Turned On A Massive, Multimillion-Dollar Moscow Surveillance System*, Forbes, published on 29th Jan. 2020, available at https://www.forbes.com/sites/thomasbrewster/2020/01/29/findface-rolls-out-huge-facial-recognition-surveillance-in-moscow-russia/;

Bryson Taylor D., *George Floyd Protests: A Timeline*, The New York Times, 18th June 2020, available at https://www.nytimes.com/article/george-floyd-protests-timeline.html;

Campbell Z. & Jones C., *Leaked reports show EU police are planning a pan-European network of facial recognition databases*, The Intercept_, published on 21st Feb. 2020, available at https://theintercept.com/2020/02/21/eu-facial-recognition-database/;

China due to introduce face scans for mobile users, BBC NEWS, published on Dec. 1, 2019, available at https://www.bbc.com/news/world-asia-china-50587098;

Clearview AI: Face-collecting company database hacked, BBC NEWS, published on 27th Feb. 2020, available at https://www.bbc.com/news/technology51658111?intlink_from_url=https://www.bbc.com/news/topics/c12jd8v541gt/facial-recognition&link_location=live-reporting-story;

Clearview AI, official website, https://clearview.ai/;

Cuthbertson A., *Indian police trace 3,000 missing children in just four days using facial recognition technology*, Independent, published on 24th Apr. 2019, available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html;

ECHR receives first complaint about facial recognition system in Moscow, TASS, published on 6th July, 2020, available at https://tass.com/society/1175141;

Ekman P., official website, https://www.paulekman.com/;

Everyday Examples of Artificial Intelligence and Machine Learning' see *https://emerj.com/ai-sector-overviews/everyday-examples-of-ai*, emerj The AI Research and Advisory Company, published on 10th Mar. 2020;

Faggella D., *AI and Machine Vision for Law Enforcement – Use-Cases and Policy Implications*, emerj The AI Research and Advisory Company, published on 20th May 2019, available at https://emerj.com/ethics-and-regulatory/ai-and-machine-vision-for-law-enforcement-use-cases-and-policy-implications/;

Fix bias in facial recognition technology, The Baltimore Sun, published on 05th Jun. 2019;

Freddie Gray's death in police custody - what we know, BBC NEWS, published on 23rd May 2016, available at https://www.bbc.com/news/world-us-canada-32400497;

Geofeedia, *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, Case Study: Baltimore County PD, 2016;

*Google, YouTube, Venmo and LinkedIn send cease-and-desist letters to facial recognition app that helps law enforcement***,** CBS NEWS, published on 5th Feb. 2020, available at https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app/;

Hartzog W., *Facial Recognition Is the Perfect Tool for Oppression*, Medium, published on 2nd Aug. 2018, available at https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66;

Haskins C., Mac R., McDonald L., *Clearview AI Wants To Sell Its Facial Recognition Software to Authoritarian Regimes Around The World*, published on 5th Feb. 2020, available at https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22;

Hernandez R., *Surveillance by default: PATRIOT Act extended?*, EDRi – European Digital rights, published on 1st April 2020, available at https://edri.org/surveillance-by-default-patriot-act-extended;

hiljade.kamera.rs: community strikes back against mass surveillance, Share Foundation, 19 May 2020, available at https://www.sharefoundation.info/en/hiljade-kamera-rs-community-strikes-back/;

Hill E., Tiefenthäler A., Triebert C., Drew J., Willis H. and Stein R., *How George Floyd Was Killed in Police Custody*, The New York Times, 19th June 2020, available at https://www.nytimes.com/2020/05/31/us/george-floyd-investigation.html;

Hill K. *The Secretive Company That Might End Privacy as We Know It*, The New York Times, published on 18th Jan. 2020, available at https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html;

Holmes A., These clothes use outlandish designs to trick facial recognition software into thinking you're not human, Business Insider, 5 Jun. 2020,

available at https://www.businessinsider.com/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10?IR=T;

Intel News, *Artificial Intelligence Explained: Unleashing the Next Wave*, published on 17th Nov. 2016, available at https://youtu.be/vehXkgG3YcU;

Jumbo Privacy Blog, *Jumbo Privacy brings a formal GDPR complaint against Clearview*, published on 14th Jul. 2020, available at https://blog.jumboprivacy.com/jumbo-privacy-brings-a-formal-complaint-against-clearview.html;

Kayser-Bril N., *At least 10 police forces use face recognition in the EU*, Algorithm Watch, published on 11th Dec. 2019, available at https://algorithmwatch.org/en/story/face-recognition-police-europe/;

Korelina O., *As Moscow's facial recognition system activates, journalists find access to it for sale on the black market*, Meduza, published on 5th Dec. 2019, available at https://meduza.io/en/feature/2019/12/06/as-moscow-s-facial-recognition-system-activates-journalists-find-access-to-it-for-sale-on-the-black-market;

'*Learning to Live with Artificial Intelligence: "A Virtuous Circle or a Vicious One?*"', International Peace Institute, published on 22nd Jun. 2018, available at https://www.ipinst.org/2018/06/governing-artificial-intelligence#5;

Mac R., Haskins C. and McDonald L., *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BuzzFeed News, published on 27th Feb. 2020, available at https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement;

Magrid L., IBM, Microsoft and Amazon not letting Police use Facial Recognition Technology, Forbes, 12 Jun. 2020, available at https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/;

Martin N., *The Major Concerns Around Facial Recognition Technology*, Forbes, published on 25th Sep. 2019, available at https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/;

Moscow has one of the world's largest CCTV systems with face recognition, mos.ru – Moscow Mayor official website, published on 29th Sep. 2017, available at https://www.mos.ru/en/news/item/30105073/;

Moscow to Deploy Facial-Recognition Tech at Rallies, The Moscow Times, published on 6th Sep. 2019, available at

https://www.themoscowtimes.com/2019/09/06/moscow-to-deploy-facial-recognition-tech-at-rallies-a67174;

New surveillance cameras in Belgrade: location and human rights impact analysis – "withheld", Share Foundation, 19 Mar. 2019, available at https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/;

New York Post, *JFK Airport's Terminal 1 launches facial recognition boarding*, published on 8th Oct. 2019, available at https://nypost.com/2019/10/08/jfk-airports-terminal-1-launches-facial-recognition-boarding/;

Oliver K. & Neenan A., *In the blink of AI: How facial recognition technology is capitalising on the COVID-19 crisis*, Euronews, published on 14 May, 2020, available at https://www.euronews.com/2020/05/14/in-the-blink-of-ai-how-facial-recognition-technology-capitalising-on-covid-19-crisis-view;

O'Sullivan D., *This man says he's stockpiling billions of our photos*, CNN Business, published on 10th Feb. 2020, available at https://edition.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html;

Privacy International, *MONITORYOU: the MilliONs being spent by the eu on developing surveillance tech to target YOU*, available at https://privacyinternational.org/long-read/3341/monitoryou-millions-being-spent-eu-developing-surveillance-tech-target-you;

Russia: Intrusive facial recognition technology must not be used to crackdown on protests, Amnesty International, published on 31st Jan. 2020, available at https://www.amnesty.org/en/latest/news/2020/01/russia-intrusive-facial-recognition-technology-must-not-be-used-to-crackdown-on-protests/;

Russia's use of facial recognition challenged in court, BBC News, published on 31st Jan. 2020, available at https://www.bbc.com/news/technology-51324841;

Sadler D., *OAIC investigates 'dangerous' face recognition app*, Innovation Aus, published on 28 Jan. 2020, available athttps://www.innovationaus.com/oaic-investigates-dangerous-face-recognition-app/;

Schoolov K., *How police use powerful surveillance tech to track George Floyd protests*, CNBC, published on 18 June 2020, available at https://www.cnbc.com/2020/06/18/heres-how-police-use-powerful-surveillance-tech-to-track-protestors.html;

Schwartz O., *Don't look now: why you should be worried about machines reading your emotions*, THE GUARDIAN, published on 6 Mar. 2019, available at https://www.theguardian.com/technology/2019/mar/06/facial-recognition-software-emotional-science;

Stanley J., *Meet Cambridge Analytica: the Big Data communications company responsible for Trump & Brexit*, published on 2 Feb. 2017, available at https://nota-uk.org/2017/02/02/meet-cambridge-analytica-the-big-data-communications-company-responsible-for-trump-brexit;

Stolton S., *After Clearview AI scandal, Commission 'in close contact' with EU data authorities*, EURACTIV, published on 12th Feb. 2020, available at https://www.euractiv.com/section/digital/news/after-clearview-ai-scandal-commission-in-close-contact-with-eu-data-authorities/;

Terrorism in the EU: terror attacks, deaths and arrests, published on 6th Sep, 2019, available at https://www.europarl.europa.eu/news/en/headlines/security/20180703STO07125/terrorism-in-the-eu-terror-attacks-deaths-and-arrests;

THALES, *Facial recognition: top 7 trends*, published 16th Feb. 2020, available at https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition;

The Guardian, NSA FILES: DECODED, published on 1st Nov. 2013, available at https://www.theguardian.com/us-news/the-nsa-files;

Tighe A., *The Australian behind Clearview AI, a facial recognition software, says it is being used here*, The World Today ABC, published on 17th Mar. 2020, available at https://www.abc.net.au/news/2020-01-23/australian-founder-of-clearview-facial-recognition-interview/11887112;

Wang M., *The Robots are Watching Us*, Human Rights Watch, published on 6th Apr. 2020, available at https://www.hrw.org/news/2020/04/06/robots-are-watching-us;

Yu K., *Facial recognition: Concerns over China's widespread surveillance*, Aljazeera, 18 Feb. 2020, available at https://www.aljazeera.com/news/2020/02/facial-recognition-concerns-chinas-widespread-surveillance-200218111532668.html;

Zlobina A., Moscow's Use of Facial Recognition Technology Challanged, *Human Rights Watch, published on 8th July, 2020, available at* https://www.hrw.org/news/2020/07/08/moscows-use-facial-recognition-technology-challenged.

Case-law

CJEU, *Digital Rights Ireland*, joined cases C-293/12 and C-594/12, 8 April 2014;

CJEU, *J.N. v Staatssecretaris van Veiligheid en Justitie,* case C-601/15 PPU, 15 February 2016;

ECtHR, *Amann v. Switzerland,* 27798/95, 16 February 2000;

ECtHR, *Bukta and others v. Hungary*, 25691/04, 17 July 2007;

ECtHR, *Ezelin v. France*, 11800/85, 26 Apr. 1991;

ECtHR, *E.B v. France*, 43546/02, 22 January 2008;

ECtHR, *Gaughran v. United Kingdom,* , 45245/15, 13 June 2020;

ECtHR, *Hasan and Chaush v. Bulgaria*, 30985/96, 26 October 2000;

ECtHR, *Huvig v. France*, 11105/ 84, 24 April 1990;

ECtHR, *Leander v. Sweden,* 9248/81, 26 March 1987;

ECtHR, *M.K. v. France*, 19522/09, 18 July 2013;

ECtHR, *Malone v. the United Kingdom,* 8691/79, 2 August 1984;

ECtHR, *N. v. the United Kingdom,* 26565/05, 27 May 2008;

ECtHR, *Plattform Arzte fur das Leben v. Austria*, 10126/82;

ECtHR, *Pretty v. the United Kingdom*, 2346/02, 29 July 2002;

ECtHR, *Rotaru v. Romania*, 28341/95, 4 May 2000;

ECtHR, *S. and Marper v. the United Kingdom*, 30562/04 and 30566/04, 4 December 2008;

ECtHR, *Unuz v. Germany*, 35623/05, 02 September 2010;

ECtHR, *Weber and Saravia v Germany* (admissibility) 54934/00, 29 June 2006;

ECtHR, *Zakharov v. Russia*, 47143/06, 4 December 2015.