Recognised and Harmed

A Classification Approach to Facial Recognition Technologies

By

Georgios Bouchagiar

Recognised and Harmed: A Classification Approach to Facial Recognition Technologies

by Georgios Bouchagiar

This book first published 2023

Ethics International Press Ltd, UK

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

Print Book ISBN: 978-1-80441-296-1

eBook ISBN: 978-1-80441-297-8

Table of Contents

Preface

This book is the result of my four-year-research (2020-2023) on biometric surveillance and privacy, as well as my six-year-experience (2018-2023) in human rights and environmental activism. Moreover, it was the basis for my PhD thesis "A Classification Approach to Face Recognition Technologies" (Ionian University 2023; PhD Committee: Prof. Maria Bottis; Assoc. Prof. Georgios Yannopoulos; Assoc. Prof. Ioannis Deligiannis; Prof. Sotiris Livas; Prof. Lilian Mitrou; Assist. Prof. Fereniki Panagopoulou-Koutnatzi; and Prof. Stavros Katsios).

My research wouldn't have been possible without the support of Silvia, Estela, Erietta, Alexandros, Nadine, Pinelopi, Lidia and Koureio's renegade thinkers.

Thessaloniki, 29 September 2023

Georgios Bouchagiar

the purposes for which private actors (potentially holders of proprietary rights) can sell face-analysing-instruments to public actors (and possibly reserve their intellectual property rights-related claims) have been neither expressly addressed nor clearly responded by regulators. Third, and as a consequence of un(der)-regulation, face recognition-implementations can lead to unprecedented surveillance-regimes; a mass-surveillance-scheme, where public actors, private entities or even citizens themselves may watch individuals or groups of people or their whatever patterns remotely and secretly for unspecified purposes and in unintelligible processing-ways.

This dark, multi-purpose and multi-way nature of contemporary face recognition-uses may threaten privacy, but also raise other human rights-concerns. More precisely, today's tech-landscape seems to have established a watching regime from which citizens may hardly hide. Even where hiding is possible or even imposed by law (by, for instance, emergency covid-related measures mandating mask-wearing), such a hiding can make the technology better in drawing more complex insights and patterns after processing fewer traits in a more sophisticated fashion.

In addition to these technological challenges, there are legal issues. Focusing on Europe, there appears to be a well-developed and well-framed legal scheme on human rights, in general, and privacy, in particular; a scheme, promising enhanced protection from risks and threats posed by any technological use. In fact, European data protection laws seem technologically neutral, providing for general processing principles that need be complied with by the duty-bearers (the data controllers or processors). Although the European approach is generic enough to cover any technological implementation, it might be too abstract, in the sense of not being targeted at concrete tech-uses, including face recognition. In addition, case law has long addressed proportionality-questions in particular relation to biometric surveillance or other intrusive practices; albeit the very ad hoc adjudication on a case-by-case basis that comes ex post (after the harm) may result in legal uncertainty. Besides, increased opacity surrounding private/public partnerships in various fields, including the exercise of secret state-surveillance via proprietary tools, can make face recognition invisible to the citizen-eye.

In light of the above considerations, there is no guarantee that the use of private face recognition technologies is adequately regulated to minimise privacy harms.

1.2 State of the art, methodology and relevance

Thus far literature has addressed various challenges posed by the impact of technological implementations on the people, in their capacity as data subjects, citizens or human beings. Well-known is Giddens and Pierson's *Risk Society* (analysed in more detail in chapter 8), accurately capturing attention overpaid to the future and its uncertainty; Lyon's *Surveillance Society* (discussed in chapters 2 and 8), reflecting on the overwatching of anyone in their whatever capacity; or Zuboff's *Surveillance Capitalism* (addressed in chapter 2 and, in more detail, in chapter 8), where the global architecture of behaviour-alterations can introduce novel risks to the very human nature. Moreover, the black-box effect of sophisticated technologies (further scrutinised in chapter 2) has been an old subject of legal discussions, in particular relation to automated processing that can be regulated by stringent data protection laws. Other flexible approaches, from collaborative governance to independent expert agencies (discussed in chapters 8 and 9), have further promised the placing of the 'data science expert' and the 'legal expert' on an equal footing.

However, to address contemporary face recognition realities, surrounded by opacity, bias and complexity, embedded within private/public decision-making procedures, rendering the people in their various legal, social or other capacity particularly vulnerable, foretelling aspects of the human (such as emotions or intent) that might make Orwellian dystopias materialised, regulators cannot rely (solely) on biopolitics and other concepts of earlier decades (such as the risk society), data protection laws that appear generic, risk-based and tech-neutral or theoretical approaches that may be hardly adopted in practice or may miss implementation-standards to ensure legal certainty.

This study builds and reflects on thus far literature and critically analyses the European legal regime, with a view to submitting a classification approach to adequately regulate the use of private face recognition technologies within the European regime and minimise privacy harms. It mainly follows a conceptual methodology entailing legal and philosophical analyses, as well as research in fields of social and political sciences. An interdisciplinary approach is adopted as a necessary means to gain a well-informed view on particular issues; new complex technological uses, for example. The primary sources used include books, journal articles, contributions to edited books, as well as legal texts, including case law.

More concretely, this study detects three crucial challenges posed by contemporary uses of private face recognition technologies: opacity (from both a legal and a technological point of view); lack of concrete checks and balances, where private face recognition technologies enter sensitive areas, especially the public realm; and the risk of mass surveillance. It further finds three regulatory challenges: vagueness of data protection law; uncertainty of ad hoc case law; and increased opacity engulfing private/public partnerships. It is submitted that the European legal regime is well-framed and tech-neutral. Although neutrality is desirable, because it can make privacy laws cover any possible technological use, neutral laws demand contextualisation to target specific uses and harms. This contextualisation can be made by courts that adjudicate on a case-by-case basis taking into due account the particularities of the tech-implementation at hand. However, case law suffers legal uncertainty, since judges engage in a case-by-case assessment that is moreover ex post (it comes after the materialisation of the harm). Other applicable legal instruments (from intellectual property-law to contract law or criminal schemes) appear to grant private entities much freedom in regulating their own technologies (via, for instance, subjection to trade secrecy protection) and public authorities much discretion in exercising surveillance via means of their choice, including private technologies. After scrutinising the European legal regime (data protection law, case law on biometric surveillance, database-law, contract law and legal provisions on cybercrime), this study claims that European regulators have failed to adequately address and particularise in an ex ante and context-dependent fashion and on a clear regulatory ground the ‘who’, the ‘what’, the ‘why’ and the ‘how’ of a given face recognition implementation.

This study argues for an acute regulatory need to focus on the ‘who’, in their concrete capacity (that is, who watches and who is watched), the ‘what’ (as input/output of a given processing operation), the ‘why’ (the goal served by a specific tech-implementation) and the ‘how’ (possible limitations of the processing-rationale, from complexity to opacity). On the ‘who’ and the ‘what’, reference is made to most recent technologies (like decentralised ledgers and forensic DNA instruments) and their regulation and practice in Europe, demonstrating that the European approach is too technical and data-focused, missing substance that is required to look at the ‘who’ (such as the citizen/state or the employee/employer, instead of the ‘data subject’ and the data controller) and the ‘what’ (like our emotions or intent, instead of ‘personal data’ or ‘biometric data’). On the ‘why’ and the ‘how’, the concept of the ‘public/private interest’ (as goals) and the complex processing (as artificially intelligent processing) are explored to make the argument that the goals pursued (ranging from broad legal concepts to unspecified purposes served by opaque tech-uses) and the dark processing (its possible opacity, bias and complexity) can be better addressed by reconceptualising the status of the actor that decides upon the goals and the way of the processing. In this regard, this study relies upon the concepts of the ‘judiciary’ and the ‘fiduciary’, sharing two key elements in common: the fiduciary obligation of reasonableness (duty to justify the decision-making) can be identified with the judge’s epistemic authority (imposing the same justification-duty); and the fiduciary obligation of fairness (requiring adherence to fair procedures) can correspond to the judge’s decisionist authority (demanding the same adherence). This study submits that the fiduciary and the judiciary approach can, in the context of legally and technologically dark face recognition-implementations, ensure optimal levels of transparency, reason-giving, fairness, accountability and other crucial principles that are desirable in sensitive areas, especially the public field.

Thereafter, it engages in a theoretical discussion on society and the human nature to critically address the ‘data society’ as a society-mode that overpays attention to the (alleged, but most probably illusory) absolute objectivity and accuracy of technologies; to prioritise utilitarian cost/benefit assessments; to pre-emptively place much emphasis on the ‘harm’ or the ‘evil’ that must be prevented; to over-deploy scarcity to exploit what would be otherwise freely available and sharable; or to confuse ‘risk’ with ‘fact’. In this context, this study argues for a human/natural society, where special focus would be placed on optimal reliability, fundamental principles and scientific readiness of technologies, vulnerability of the watched and sensitivity of what is to be processed and/or predicted, desirable freedom of technologies and their users and whether and the degree to which risk may be relied upon. To this end, this study addresses scientific and legal dimensions of reliability (known from statistics, evidence law and case law-standards); the logic of the ‘fundamental’ vis-à-vis utilitarian cost/benefit approaches and assessments; vulnerability of those meriting protection and sensitivity of data subjectable to face recognition (the ‘good’ to be protected versus the data society’s ‘evil’ to be prevented); desirability to have a given technology freed from or, contrary, subjected to proprietary schemes (instead of blindly imposing scarcity to benefit financial interests, as we have learned from intellectual property-discussions); and whether and the extent to which risk can/must be relied upon, avoiding over-trusting and over-relying upon likelihoods, as 'facts' or something 'given', to make future claims.

To overcome challenges posed by the 'data society', this study proposes the concept of the 'natural society'. Seeing nature as a human-independent landscape, where human observers perceive natural (human-independent) ideas and transfer them into societies, it claims that, upon human perception, these ideas gain subjectivity and, therefore, any human society can entail the logic of the 'subjective'. This logic is, the argumentation goes, disregarded by the 'data society' that sees people, not as humans in their natural environment but, as data, items of information bearing a label corresponding to a group (hardly existing in reality, such as the 'rational citizen'). Finding that the 'data society' goes against both the nature and the human and this may be the reason for its future failure, it suggests a regulatory architecture relying upon the above human seek for natural ideas and the transferring of these ideas into reality (societies) and their subjectification.

More concretely, this study recommends the introduction of an independent expert agency that would ex ante (upon request of the tech-designer or other stakeholder, including public entities, and before a given face recognition implementation) engage in a two-step process, that would be context-dependent and regulation-based. After specifying the 'who', the 'what', the 'why' and the 'how' of the face recognition technology at hand, the agency would, first, identify the fundamental principles (natural ideas) that need be respected, as well as applicable laws mandating respect for these principles; and, second, it would strike a fair balance between possibly conflicting stakes (rights and freedoms), particularise and specify what the principles identified (in the first step) mean in the specific context (where face recognition is to be applied) and, finally, engage in five fundamental assessments addressing: reliability of the technology; its scientific readiness to enter the field, as well as its potential to comply with principles detected; vulnerability of those to be protected and sensitivity of the patterns to be processed/predicted; desirability of freedom or, contrary, subjection to proprietary schemes; and risk-reliance (whether and the extent to which risk can/must be trusted in reaching a decision). After this two-step scrutiny the agency would classify the face recognition use at hand; it would reject or accept its use in the field; and it would rule on whether and how face recognition uses, falling in the same category in which the technological implementation under assessment would be sorted, can be allowed. This classification-task, namely the ruling of the agency, could then be embedded within existing laws, thus offering concreteness and detailedness in the law, legal certainty in the balancing exercise and optimal transparency and justifiability where sensitive areas demand so.

1.3 Overview of chapters

Chapter 2 aims address whether and to what degree the use of private face recognition technologies can interfere with privacy. It first defines private face recognition technologies, in a broad way, to include tools that are designed, controlled or used by private entities, involve face-related data as input and/or output and offer a probability that a person or a group or their face-related or other patterns can be recognised. This broad definition is imperative to cover technologies, which, though seemingly irrelevant to the 'face' and its 'recognition', do involve aspects of the 'face' or the 'recognition' task; for instance, DNA phenotyping is not aimed at recognising someone's face (in the narrow sense), but it can input face-related data (like hair or saliva) and output the likelihood that the DNA-owner may have brown eyes or black hair.

Thereafter, chapter 2 detects three key challenges, stemming from the use of private face recognition technologies. First, it analyses opacity from a technological and a legal point of view. Technological opacity can refer to complexity of contemporary sophisticated technologies; and legal opacity is concerned with proprietary claims raisable by private actors (such as trade secrecy). Reference is made to concrete examples and cases, demonstrating that private face recognition technologies have become ubiquitous and entered any area, including the public realm. This poses the second crucial challenge: lack of concrete and enhanced checks and balances to ensure that transparency, reason-giving and other fundamental principles, mandated by public law, are respected, where private tools enter public fields. Exploring how developments in law and technology have resulted in a rather police-friendly scheme, necessitating analogous citizen-shielding safeguards and precautions, this chapter addresses the third challenge of mass surveillance; a monitoring-mode that goes beyond old-school 'control from above' to include various intrusive practices, from identity-establishment to gaining knowledge about groups or investigating conducts, that may be engaged in by both public and private actors.

Having submitted in detail the three risks posed by the use of private face recognition technologies, chapter 2 discusses privacy from a theoretical perspective. The concept of 'privacy' is understood broadly to include its multiple dimensions and, in particular, its positive and negative aspects, its manifestation in both private and public spaces and, importantly, the overarching type of 'informational privacy'. This broad approach allows for the detection of concrete privacy dimensions that may be interfered with by specific surveillance-modes. Chapter 2 concludes that the use of private face recognition technologies can heavily interfere with informational privacy (the right to deny access to and to enjoy and maintain control over personal information) and to a considerable degree with behavioural privacy (especially, the right to remain anonymous), associational privacy (the right to associate with peers) and intellectual privacy (the right to develop personality and ideas).

Thereafter, chapters 3 to 7 aim to detect the regulatory challenges of subjecting the use of private face recognition technologies to the European framework. Chapter 3 analyses the European legal regime and finds three key regulatory challenges: abstractness in the law; uncertainty in case law; and increasing opacity in the exercise of surveillance by private/public partnerships. The study then claims that there is a pressing need for ex ante, regulation-based and context-dependent face-recognition-rules that would take into due account the 'who' (chapter 4), the 'what' (chapter 5), the 'why' (chapter 6) and the 'how' (chapter 7).

More concretely, chapter 3 focuses on the European legal approach to the right to privacy and the protection of personal data. It refers to both the Council of Europe and the European Union and investigates the legal instruments that are applicable to the use of private face recognition technologies. The analysis demonstrates that the European legal scheme is well-framed, generic, abstract and technologically neutral. This may be positive, as possibly covering any existing or emerging technological use. However, it seems to lack clarity and detailedness, when it comes to specific implementations and, in particular, face recognition. The latter is put under the broad umbrella of biometrics (as special category of personal data), which (as chapter 3 claims) may suffer definitional inadequacies.

In addition, the legal analysis scrutinises case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) on biometrics and surveillance. The discussion focuses, on the one hand, on the regular proportionality-tests performed by the two courts, where a privacy-interference has been established; and, on the other hand, on biometric surveillance-cases. This case law-scrutiny demonstrates that the courts' case-by-case assessment that comes ex post (after a privacy-interference has occurred and been established) may result in legal uncertainty. There is no standard criterion to specify and particularise, among others, the level of protection that the various categories of biometrics merit or the surveillance-modes that may be tolerated or, contrary, prohibited.

The legal discussion moves on to other European legal tools that may be relevant for and applicable to the use of private face recognition technologies. These legal instruments include, on the one hand, proprietary protection granted by database-related law, contract law, as well as trade secrecy; and, on the other hand, protection offered by substantive and procedural criminal law on cyber-crime. The analysis of the former proprietary tools shows that private entities may enjoy unfettered discretion in regulating their own technologies and secretly directing them to whatever purposes; this may have a particularly hostile impact on citizens, especially where opaque face recognition enters sensitive areas, like the public arena, where enhanced checks and balances must be in place. The lack of such enhanced checks and balances is also proven by the analysis of the legal provisions on cybercrime, which may leave specific technological implementations un(der) regulated. In this regard, chapter 3 addresses police hacking as a surveillance-mode, where law enforcement is given much discretion in exercising secret surveillance via private technologies that can include face recognition.

Having analysed applicable law and case law, chapter 3 finds the above three key regulatory challenges of subjecting the use of private face recognition technologies to the European framework: vagueness of law; uncertainty of case law; and potential undesirable results of proprietary protection or other types of protection establishing secret public/private partnerships that may escape enhanced checks and balances. Taken together, the law's technological neutrality and vagueness, case law's uncertainty due to ex post ad hoc assessments and alarmingly increasing opacity in the exercise of surveillance by public/private partnerships create an acute need for face recognition-targeted rules that must be ex ante, regulation-based and dependent on the context; namely, the 'who', the 'what', the 'why' and the 'how' of concrete face recognition implementations.

Chapter 4 focuses on the 'who'; that is, the potential recogniser and the possible recognised, both in their concrete capacities. It argues that Europe pays special attention to (the broad concepts of) 'data controllers' and 'data subjects' and approaches these actors from a rather technical and data processing perspective, missing substance. This may lead to uncertainties and raise accountability-related concerns, especially where complexities of contemporary technologies may blur the distinguishing line between duty-bearers and rightsholders. To support this argument, this chapter discusses Distributed Ledger Technologies (DLTs) and their intrinsic and emergent features vis-à-vis case law (of the CJEU) and soft law on joint controllership. It concludes that there is a pressing need to properly identify the 'who' in their concrete (social, legal or other) capacity; and this, not (solely) from a technical perspective, but (primarily) in a context-dependent fashion. It is submitted that this can be achieved through embedding face recognition-provisions within existing legal tools (like labour law codes or codes of criminal procedure).

Then, chapter 5 analyses the 'what'. It claims that contemporary uses may go beyond the 'face' of a person, who may be recognised, singled out from a data protection point of view. Today's technologies may be aimed at predicting patterns concerning groups, not individuals, and at fulfilling goals other than identification, such as the likelihood that a group of people shares common facial patterns or traits. Reference is made to Forensic DNA Phenotyping (FDP) as a technology, involving such 'face recognition' (beyond 'face' and 'recognition'), entailing exercise of surveillance by both private and public actors and interfering with various aspects of privacy. After analysing the seriousness of the interference, this chapter moves on to FDP practice and regulation in Europe. The discussion on three states (the Netherlands, Germany and Slovakia) that have concrete FDP-provisions reveals that some minimum safeguards are in place to protect citizens from possible FDP-abuse by investigating authorities; but also that, in the absence of targeted laws (where FDP is practiced, but not expressly regulated), there is legal uncertainty, especially with regard to the principles of proportionality and legality. In conclusion, chapter 5 stresses the need to attribute special weight to the 'what', to (personal or group) data as input and output of a given technology in the specific context (not only from a data protection technical perspective). Such proper weight can be given by ex ante rule-making addressing in the specific legal context sensitivity of certain patterns, as well as desirability or undesirability of certain predictions that might lead to Orwellian dystopias.

Chapter 6 is concerned with the ‘why’. The argumentation goes as follows: people make laws to regulate human affairs; these affairs by necessity entail data; hence, privacy and data protection laws are applicable to any affair. Yet, addressing any human affair by reliance upon (solely) data protection laws may not always be the proper way to regulate; especially where face recognition uses may not be targeted at privacy as such or data as such, but can have a multi-purpose nature, requiring the detection of the goal(s) served on a case-by-case basis. In this context, chapter 6 analyses the concepts of the ‘private interest’ and the ‘public interest’. It makes reference to the right to privacy, as protected under the Hellenic legal regime, to highlight that, even though there can be harmonisation at national level and states may adopt more or less similar approaches to privacy, the broadness and the multi-dimensional nature of privacy and the discretion granted to judges (performing balancing tasks) can lead to legal uncertainty. Moreover, this chapter addresses the ‘public interest’ as a concept sharing key elements with the fiduciary-notion. This can allow for the conceptualisation of public actors as fiduciaries of the people; namely, as entities that must exercise other-regarding power (power that regards the people as beneficiaries). It claims that the fiduciary approach to the watcher can overcome uncertainties, stemming from the broadness of the ‘public/private interest’ and case law’s ad hoc assessments, in light of the fiduciary duty of reasonableness (to justify decision-making) and the fiduciary duty of fairness (to adhere to fair procedures). In conclusion, chapter 6 argues for the need to impose (by ex ante rule-making) concrete fiduciary-related duties on relevant actors, who must pay special attention to and fairly justify the ‘why’.

Furthermore, chapter 7 examines the ‘how’. It claims that contemporary dark processing realities can entail opacity, bias and complexity. It is submitted that these limitations are not adequately addressed by the European regime that has adopted a rather permissive and risk-oriented approach to risky uses of artificially intelligent technologies; this approach may, chapter 7 finds, disregard the logic of the ‘fundamental’. After arguing that today’s opaque technological uses may hardly be accessed and effectively challenged by citizens, this chapter draws analogies between limitations of the technology and limitations of the human mind that is also (believed to be) opaque, biased and complex. It then suggests a human-approach to technologies and, in particular, subjection of technological processing to schemes known from the judiciary and aimed at minimising the limitations of opacity, bias and complexity. Here, the judge is addressed as both a human (carrying bias) and an authority, which must adequately justify its decision-making (as epistemic authority) and adhere to fair procedures (as decisionist authority). It is established that this two-fold (epistemic/decisionist) authority can enable judges to reach optimal rationality. Therefore, chapter 7 concludes that, in specific face recognition contexts, concrete epistemic- and decisionist-related obligations can be imposed (via ex ante rule-making) to ensure optimal justifiability, visibility and impartiality.

Having clearly responded to questions on face recognition's regulatory challenges (namely, vagueness of law, uncertainty of ad hoc case law and increasing darkness surrounding private/public partnerships) and (having) explained and established in detail the pressing need for ex ante, regulation-based and context-dependent face recognition-rule-making that must adequately consider the 'who' in their concrete capacity, the 'what' as input and output, the 'why', the goal pursued and fairly justified, and the 'how' (the possible darkness), this study moves on to the next challenges.

Chapter 8 prepares the ground for the recommendation of the classification approach (chapter 9) that would address the above challenges. Arguing for the need to reconceptualise the 'society' and the 'human nature', it uses the term 'data society' to refer to contemporary society-modes, where mass, fast and complex processing of data has resulted in a regime, where attention overpaid to the recording and the prediction of likelihoods can confuse 'risk' with 'fact', 'unknowable future' with 'known reality'. It identifies five critical points of confusion and misleading: optimal reliability (versus data society's alleged absolute accuracy); readiness of a technology and the principles to be respected (versus data society's tendency to engage in mere cost/benefit assessments before introducing new technologies); vulnerability of those affected and sensitivity of patterns to be predicted (versus data society's pre-emptive focus on the harm to be prevented); desirable freedom (versus data society's over-reliance on scarcity to exploit and limit otherwise unlimited and free goods); and diligent consideration of risk when taking decisions (versus data society's heavy reliance upon risk). This chapter recommends five fundamental assessments of reliability, readiness/principles, vulnerability/sensitivity, freedom and risk-reliance that could be conducted ex ante, be based on a regulatory ground and duly consider the 'who', the 'what', the 'why' and the 'how' of a given face recognition implementation. In its conclusion, chapter 8 claims that the proposed assessments need be fundamentally approached and dynamically performed by collaborating experts from various disciplines to guarantee that we, as humans evolving in nature and society, will: remain free and independent thinkers (instead of being rendered pre-programmed entities engaging in mechanical processing); embed desired values that respect nature-shielding principles; pay attention to the 'good' that must be protected as vulnerable and sensitive (instead of solely looking at the 'bad thing' that must be prevented); see scarcity as a last resort and abolish 'dumb' and unreasonable scarcity; and understand the notion of 'risk' and the weight attributable to it when making decisions.

Last comes chapter 9, proposing a classification approach to the use of private face recognition technologies. Addressing society from a natural point of view, it claims that nature can be seen as a (human-independent) landscape, where humans observe their surroundings and perceive natural ideas; and that these human-independent natural ideas can, upon human perception, gain subjectivity. It then argues that the data society seems to disregard the logic of the 'subjective'. It, thus, suggests moving away from the data society and toward the 'natural society'. The latter could rely on a regulatory scheme based on the above nature-landscape-notion and the human quest for natural values. More concretely, chapter 9 proposes the introduction of an independent expert agency that would engage in a two-step scrutiny (before a given private face recognition technology enters the field). After detecting the 'who', the 'what', the 'why' and the 'how', the agency would, first, identify the fundamental principles and the legal provisions that seem applicable to the specific face recognition use (under scrutiny). Second, the agency would strike a fair balance between possibly conflicting stakes, particularise the fundamental principles (what these principles mean and how they can be interpreted in the concrete context) and engage in the fundamental assessments of reliability, readiness/principles, vulnerability/sensitivity, freedom and risk-reliance. After having finalised this two-step scrutiny, the agency would classify the face recognition use under examination, accept or deny that use and make a ruling covering face recognition implementations that would fall in the same group as that of the one under examination. In conclusion, chapter 9 argues that the proposed ex ante, regulation-based and context-dependent classification approach to the use of private face recognition technologies can: adequately address the regulatory challenges of abstractness in the law, uncertainty of ad hoc case law and increasing opacity in private/public partnerships;

sufficiently respond to the need for beforehand- and regulation-based rule-making that fairly considers the ‘who’, the ‘what’, the ‘why’ and the ‘how’ depending on the context; and, therefore, adequately regulate the use of private face recognition technologies within the European regime to minimise privacy harms.

Chapter 10 summarises and further discusses potential limitations of the proposed scheme.

2. Private Face Recognition Technologies Interfering with Privacy

2.1 Introduction

Private face recognition technologies are used in various contexts and for multiple purposes. This chapter examines the ways in which these technologies can be implemented and how their use may interfere with privacy. More concretely, it sees private face recognition technologies as instruments that are developed, used or controlled by private actors and which input/output face-related data (alone or in conjunction with other data) in an automated fashion with a view to calculating the probability that a person or a group or their face-related (or other) patterns may be recognised. Moreover, it discusses key challenges posed by their implementations with the objective of detecting the aspects of privacy that may be more seriously interfered with.

Part 2.2 provides for a definition of these technologies, via explaining the terms 'private', 'face', 'recognition' and 'technology'. That these instruments are private means that they can be developed, used or owned by a private actor that can enjoy discretion in designing its model, subject it to intellectual property rights protection, but also escape enhanced checks and balances (like minimum levels of transparency) known from public law and solely binding authorities performing public functions. The term 'technology' is put in contemporary processing-realities to make the argument that face recognition analysis can be conducted in an automated manner, not fully human-driven. In addition, the task of 'recognition' is understood broadly to cover, not only identification/authentication tasks typically performed by old-school face recognition but also, tasks involving face or other data as input/output to make predictions related to individuals or groups or their face-related or other patterns (for instance, DNA phenotyping, analysed in chapter 5, recognising the likelihood that someone may develop a genetic disease). Last, the 'face'-analysis demonstrates that facial information, analysed solely or in conjunction with other data to make claims on a person or a group or their facial or other patterns, can be particularly sensitive.

Controlled, used or owned by private entities, analysing sensitive data (often in combination with other items of information) in an automated fashion and offering probabilities relating to an individual or a group or their face-related or other patterns, private face recognition technologies can raise three serious concerns. First, there is legal and technological opacity. On the one hand, private face recognition technologies, trained on Big Data and exploiting new forms of Artificial Intelligence (AI), can process information in a complex, data driven manner, making their modus operandi unintelligible to humans ('technological opacity'). On the other hand, private owners, developers or controllers of face recognition technologies can subject their products to intellectual property rights and, hence, deny access to their tools ('legal opacity'). The cases and examples analysed in this chapter demonstrate that legally and technologically opaque face recognition tools can enter any domain, including the public sphere. This poses the second challenge: namely, the absence of enhanced checks and balances, where dark technologies enter the public arena. After discussing technological developments vis-à-vis trends in criminal law and procedure, highlighting the crime-nature of today's society, the police-friendly and citizen-hostile environment calling for concrete safeguards, the analysis moves on to the third challenge: mass surveillance. Private face recognition technologies can be targeted at surveilling; from controlling the people to processing their information to establish identities, gain knowledge, create groups or investigate behaviour.

This legally and technologically opaque, un(der)regulated and multi-surveillance scheme necessitates an examination of compliance with privacy. The latter is approached by part 2.3 from a theoretical perspective to assess which privacy-dimensions may be more seriously interfered with by contemporary uses of private face recognition technologies. After addressing positive and negative aspects of privacy, this part finds that informational privacy and, to a considerable degree, intellectual, associational and behavioural privacy, can be more heavily disrespected by contemporary face recognition implementations and the use of these technologies for various surveillance goals.

Last, part 2.4 summarises, draws conclusions and stresses the need to delve into legal aspects of privacy and, in particular, the right to privacy and the protection of personal data protected under the European legal framework (passing the baton to chapter 3).

2.2 The use of private face recognition technologies

To better comprehend what private face recognition technologies are about and, hence, what their effect to and impact on the people at whom they may be targeted can be, it is useful to delve into the very terminology: 'private'; 'face'; 'recognition'; and 'technology'.

Starting with the latter, 'technologies' can be seen as instruments that people use to alter or adjust to their surroundings.[1] They can be regarded as human-made tools, aimed at serving human needs. Face recognition technologies can in fact benefit a wide range of domains, from cashless payments to fast verification of a bank's client. They can do so, thanks to their automated functioning; that is, the conducting of processing operations that can be neither fully human-driven nor entirely human-guided. Rather, automated procedures can allow for data-driven processing of information; a processing, which even human experts may not be capable of explaining and comprehending.[2] Therefore, even though technology as such can be seen as an artefact, a human-made instrument, processes followed, outputs given, or decisions made by the technology itself may be tech-made; meta-artefacts created by human-made tools.

Moving on to the very task, 'recognition' has been connected with various practices, from identifying a person (for example, I 'recognise' the suspect as the person who attacked me) to respecting or taking something as given (for instance, I 'recognise' her expertise).[3] In the face recognition context, what appears to be relevant is that a person or a group or their face-related (or other) patterns 'can be recognised'. The phrasing 'can be' is preferred over the term 'is' to stress the probabilistic nature of processing operations. A face recognition technology can output a probability that there is a (for instance, 90%) likelihood that the person concerned (for instance, caught by a camera) can match a known template (like a concrete profile stored in a police database).

[1] Bert-Jaap Koops, 'Ten Dimensions of Technology Regulation: Finding your Bearings in the Research Space of Emerging Technologies' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf 2010) 309.

[2] See, in general: Woodrow Barfield, *The Cambridge Handbook of the Law of Algorithms* (Cambridge University Press 2020); Alan Rubel, Clinton Castro and Adam Pham, *Algorithms and Autonomy: The Ethics of Automated Decision Systems* (Cambridge University Press 2021).

[3] See in general: Michael Inwood, *A Hegel Dictionary* (Blackwell 1992) 245ff.

Then comes the ‘face’. Our ‘face’ can be regarded as the most crucial part of the human body when interacting with the world.[4] It is essential to externalise our inner world, but also to internalise outside environments. Our eyes are believed to be the ‘window of the soul’. When open, they can let information in, as well as out. Not only they can reveal to others what we feel, from anger to joy; they may also enable us to see our surroundings and introduce us to novel grounds. Explorers, from astronauts to water divers, would hardly enjoy or make sense of their investigative trip, if they were unable to see what their environment consists of. Or our mouth and its expressions are of utmost importance for any kind of communication, from professional conversations to intimate interactions. We use our mouth to talk and express ideas, thoughts or beliefs to our colleagues; and a kiss on the lips is crucial to receive or give love. Undoubtedly, any facial trait can play its role when interacting with others and the environment. And, admittedly, any technology capturing or otherwise processing facial traits, geometry or expressions can reveal to its owner, user or controller a variety of sensitive information. It is imperative to stress that contemporary face recognition tools can ‘recognise’ the ‘face’, but can go beyond the ‘face’ and its ‘recognition’; facial data can be involved as an input or as an output or as both; they may be analysed (alone or in conjunction with other data) to output a likelihood that a person or a group or their face-related (or other) patterns may be recognised.

Last, the term ‘private’ refers to natural or legal entities, other than public actors. The distinguishing line appears to be whether and the extent to which a given technology is designed, developed, used and/or owned by a private actor. The distinction is important, because private entities enjoy broad discretion in designing their models, as well as in subjecting them to proprietary rights protection. In addition, private actors are, in principle, not subjectable to enhanced checks and balances (like minimum levels of transparency, reason-giving, accountability or fairness) known from public law and, in principle, binding state actors.

In light of the above considerations, private face recognition technologies are, for the purposes of this study, understood broadly as tools, which involve face-related data as an input and/or as an output and, in particular, tools that: are designed, controlled, used or owned by private entities;

[4] A discussion in: Bart van der Sloot, ‘Editorial’ (2020) 6(2) European Data Protection Law Review 165.

process (often sensitive) data (including face-data) in an automated, data-driven fashion; and offer a probability, a likelihood that a person or a group or their face-related or other patterns can be recognised.[5]

The above understanding and features of private face recognition technologies, entailing automated processing of often sensitive information by private entities with a view to assessing recognisability of a person or a group or their facial or other patterns, pose three crucial challenges: legal and technological opacity; lack of enhanced checks and balances; and the threat of mass surveillance.

2.2.1 Challenge #1: Legal and technological opacity

Technological opacity leading to unintelligible data processing

Technological opacity refers to contemporary processing operations that appear particularly complex and sophisticated, hardly comprehendible by human experts. To better understand this type of opacity, it is helpful to discuss the technological context, in which face recognition technologies function: Big Data and AI.

The term 'Big Data' refers to the complex and rapid processing of vast amounts and wide range of information with a view to foretelling patterns. Gigantic datasets are analysed to predict future situations on the grounds of data driven decisions;[6] decisions relying on data analysis, rather than human intuition.[7] The data driven rationale and predictive function of Big Data can allow for novel discoveries, not obvious to humans, that may turn out to be particularly valuable for purposes pursued.[8]

[5] For similar definitions and the EU approach to face recognition technologies, see: European Data Protection Board, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement' (Version 1.0, adopted on 12 May 2022) <https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf>.

[6] Danah Boyd and Kate Crawford, 'Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon' (2012) 15(5) Communication & Society 662, 663.

[7] Foster Provost and Tom Fawcett, 'Data Science and its Relationship to Big Data and Data-Driven Decision Making' (2013) 1(1) Big Data 51, 53.

[8] Dennis Broeders and others, 'Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data' (2017) 33(3) Computer Law & Security Review 309, 312.

However, undesirable risks may emerge. The forecasting function, based upon probability-oriented approaches, does not allow for undoubtful knowledge.[9] Moreover, decisions, driven by and based on data, imply too much discretion left to technologies in deciding how to process inputs. Such processing may be completely opaque and unintelligible, where new types of artificially intelligent technologies learn from experience and engage in complex analysis.[10] Although there are novel forms of AI that may

transform contemporary processing operations into a black box, the rationale underlying AI, that is to make machines act as if they were clever humans, is not new.

From time immemorial to the era of Big Data, humans have been endeavouring to transfer their attributes to technology for various reasons. In ancient polities, they gave statues voice conveying messages of gods; statues became a tool to persuade ignorant audiences.[11] In mechanised civilisations of the eighteenth century, they gave technology muscle powers and delegated tasks that were hard for them to carry out.[12] In more modern societies of the mid-twentieth century, they claimed transmission of intelligence;[13] and, today, humans are accused of having transferred opacity, bias, complexities and other traits of their mind[14] that are said to contribute to imperfection, a crucial source of their (alleged) freedom.[15]

During the twentieth century's debates on the name of AI, 'artificial intelligence' was favoured over 'complex information processing'.[16] The

[9] Eyal Amir, 'Reasoning and Decision Making' in Keith Frankish and William Ramsey (eds), *The Cambridge Handbook of Artificial Intelligence* (Cambridge University Press 2014) 191, 202, 209.

[10] Michael Butterworth, 'The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework' (2018) 34(2) Computer Law & Security Review 257, 259.

[11] Noel Sharkey and Amanda Sharkey, 'Artificial Intelligence and Natural Magic' (2006) 25(1-2) Artificial Intelligence Review 9, 10.

[12] Benny Karpatschof, 'Artificial Intelligence or Artificial Signification?' (1982) 6(3-4) Journal of Pragmatics 293, 295.

[13] See among others: Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford University Press 2014).

[14] See generally: Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing Group 2016).

[15] Yochai Benkler as cited in: Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton 2015) 116.

[16] Herbert Simon, 'Artificial Intelligence: An Empirical Science' (1995) 77(1) Artificial Intelligence 95, 96.

latter could capture more accurately AI’s goal to make unintelligibility intelligible, render intelligence comprehensive. However, the former was more popular;17 and it could very well illustrate the same goal, understood from a rather engineering point of view as the purpose of making machines engage in acts that would be deemed intelligent, if carried out by humans.[18]

The history of AI reveals with clarity that the greatest developments in directing technologies toward fulfilling this goal were taken forward during the mid-twentieth century. In that era, experts made their best efforts to well-define AI; enhance its performance through tests passed by promising technology tricking humans it is a human; or build systems that represented and interpreted their surroundings, learned from these surroundings and used knowledge acquired to achieve goals pursued.[19] These efforts allowed for insights into intelligence itself, the human mind and the technology. AI-experts endeavoured to capture human mind that entailed something more complicated than mere ‘if/then’ syllogisms suggested by simplified deductive reasoning.[20] To illustrate this ‘something more complicated’, they designed artificial neural networks; nets that can be seen as the predecessors of today’s deep learning technologies making computers win human champions in narrow tasks, such as board games (for example, chess or ‘Go’).[21]

Put simply, AI-technologies that people use today, from algorithms to networks, date back to the previous century.[22] What seems to be new is the phenomenal rate at which datasets and processing power have grown and continue to grow. This can be seen as the twofold bigness of Big Data, the environment upon which AI can be trained. On the one hand, gigantic

[17] A discussion in: Herbert Simon, ‘Artificial Intelligence’ (n 16) 95ff.

[18] Marvin Minsky, *Semantic Information Processing* (MIT Press 1969) v.

[19] For an overview of the four seasons of AI, see: Michael Haenlein and Andreas Kaplan, ‘A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence’ (2019) 61(4) California Management Review 5.

[20] A comprehensive discussion on machine reasoning in particular relation to logic and deduction, in: Matt Carter, *Minds and Computers: An Introduction to the Philosophy of Artificial Intelligence* (Edinburgh University Press 2007) 132-144.

[21] Michael Haenlein and Andreas Kaplan, ‘A Brief History of Artificial Intelligence’ (n 19) 8.

[22] Lilian Edwards and Michael Veale, ‘Slave to the Algorithm? Why a ‘Right to an Explanation’ is Probably Not the Remedy You Are Looking For’ (2017) 16(1) Duke Law & Technology Review 18, 25.

datasets are subjected to analysis; and, on the other hand, this analysis entails unprecedentedly fast and sophisticated processing with a view to making optimally accurate estimates. The result is technological opacity: complex processing hardly explainable to or by human experts.

Legal opacity: legitimate denial of access

While technological opacity refers to complexities in technical aspects and environments of the processing operations, legal opacity is linked to legitimate denial of access, in light of property rights set out by law. More concretely, intellectual property rights can include a wide variety of sub-rights, ranging from patents or copyright to trademarks, database rights or trade secrets.[23] These rights can subject items of information to legal claims, such as the right to exclude someone from using a musical work or the right to make financial profits via the exploitation of undisclosed data (like a trade secret). Although each sub-category of intellectual property rights can have its own foundations, justifications or approaches, all of them appear to reflect one common thing: human's endeavour to grasp often intangible information with a view to expanding knowledge and ultimately benefiting arts or sciences. This endeavour has long been addressed and represented through the 'data-information-knowledge-wisdom' pyramid.[24]

More concretely, information is something fundamental.[25] Same as many concepts, what information is or means may context-dependent.[26] For

[23] See, in general: Justine Pila and Paul Torremans, *European Intellectual Property Law* (Oxford University Press 2016).

[24] See, among others: Jennifer Rowley, 'The Wisdom Hierarchy: Representations of the DIKW Hierarchy' (2007) 33(2) Journal of Information Science 163, 164.

[25] James Gleick, *The Information, A History, A Theory, A Flood* (Pantheon Books 2011) 8. For definitional challenges, see: Cornelis van Rijsbergen and Mounia Lalmas, 'Information Calculus for Information Retrieval' (1996) 47(5) Journal of The American Society for Information Science 385; Joseph Goguen, 'Towards a Social, Ethical Theory of Information' in Geoffrey Bowker and others (eds), *Social Science Research, Technical Systems and Cooperative Work: Beyond the Great Divide* (Erlbaum 1997) 27, 27-28; Mark Burgin, 'Information: Problems, Paradoxes, and Solutions' (2003) 1(1) tripleC 53, 57.

[26] Rafael Capurro and Birger Hjørland, 'The Concept of Information' (2003) 37 Annual Review of Information Science and Technology 343, 344, 396; Luciano Floridi, 'Is Semantic Information Meaningful Data?' (2005) 70(2) Philosophy and Phenomenological Research 351, 352.

Coming from Latin, 'datum' can be understood as 'something given'.[37] In the old times, a popular use –in the feminine form– was 'epistola data', that is 'letter delivered' or 'letter given'; this is believed to have led to the use of 'date' in letters.[38] In its early use in mathematics, 'data' referred to something that was recognised as the grounds, the basis to make a claim.[39] It referred to an assumption or a 'fact', 'something done'.[40] In later uses in other fields, 'data' could refer to the outcome of experiments.[41] Today, experts treat the term as a representation or a description of something that enables it to be recorded and processed.[42] This could include previous understandings of data. In fact, in contemporary complexities of Big Data analysis, a datum could be seen as a given ground but also as the result of an investigation.

For example, a user may enter her name, phone number and email when using a social networking platform. Such data may be stored and analysed and, therefore, become the basis to make claims. Private technologies can use these data as the grounds to discriminate for or against users.[43] At the same time, data may be the result of an experiment. For instance, one's health condition (as data) could be seen as the outcome of her shopping behaviour ('experiment' or 'investigation'). This was the case with Target, a firm that investigated consumers' behaviour to predict the outcome; in that case, pregnancy.[44] Target had identified certain commercial products that, when bought together, indicated that the purchaser was likely to be pregnant. After having perused what individuals had been purchasing,

[37] Cornelius Puschmann and Jean Burgess, 'Metaphors of Big Data' (2014) 8 International Journal of Communication 1690, 1691; Lee Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight' (2015) 35(1) Oxford Journal of Legal Studies 91, 113; Daniel Rosenberg, 'Data Before the Fact' in Lisa Gitelman (ed), *"Raw Data" Is an Oxymoron* (The MIT Press 2013) 15, 18.

[38] Vivian McAlister, 'Datum Isn't; Data Are' (2016) 59(4) Canadian Journal of Surgery 220.

[39] Daniel Rosenberg, 'Data Before the Fact' (n 37) 32-33.

[40] Michela Cennamo, 'The Rise and Grammaticalization Paths of Latin Fieri and Facere as Passive Auxiliaries' in Werner Abraham and Larisa Leisiö (eds), *Passivization and Typology: Form and Function* (John Benjamins Publishing 2006) 311.

[41] Daniel Rosenberg, 'Data Before the Fact' (n 37) 33.

[42] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform how We Live, Work, and Think* (Houghton Mifflin Harcourt 2013) 78.

[43] Latanya Sweeney, 'Discrimination in Online Ad Delivery' (2013) 11(3) Queue 1.

[44] Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55(1) Boston College Law Review 93, 94ff, 98ff.

the firm accurately foresaw that a consumer was pregnant. Similar examples may include cases where technologies, based on people's habits, may predict drug use[45] or the likelihood of cancer.[46]

In the era of 'data explosion',[47] 'data tsunamis' and 'data mountains',[48] datafication can enable anything, even people and their emotions, to be recorded and analysed and, thus, become data.[49] However, not everything can (or is supposed to) have meaning.

Meaning, the second element of the above definition of information, has been associated with analysing, explaining or interpreting something to understand it.[50] Namely, it has been related to ways in which humans use language to comprehend and make sense of their surroundings.[51] From this perspective, meaning seems to need experience that could result in some form of perception.[52] The latter could be translated into language, words

[45] Michal Kosinski, David Stillwell and Thore Graepel, 'Private Traits and Attributes are Predictable from Digital Records of Human Behavior' (2013) 110(15) Proceedings of the National Academy of Sciences of the United States of America 5802.

[46] Anthony Casey and Anthony Niblet, 'The Death of Rules and Standards' (2017) 92(4) Indiana Law Journal 1401, 1424ff.

[47] Christophe Geiger, Giancarlo Frosio and Oleksandr Bulayenko, 'Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data?' (2018) 49(7) International Review of Intellectual Property and Competition Law 814, 815.

[48] Andreas Stylianou and Michael Talias, 'Big Data in Healthcare: A Discussion on the Big Challenges' (2017) 7(1) Health and Technology 97, 99.

[49] Deborah Lupton, 'Personal Data Practices in the Age of Lively Data' in Jessie Daniels, Karen Gregory and Tressie McMillan Cottom (eds), *Digital Sociologies* (Policy Press 2017) 339, 341ff; Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data* (n 42) 73ff; Jörg Lehmann and Elisabeth Huber, 'Lost in Datafication? - A Typology of (Emotion) Data Contextualization' (2018) Integrative Psychological and Behavioral Science 1; Alessandro Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34(4) Computer Law & Security Review 754, 761.

[50] Yair Neuman, 'Meaning-Making in the Immune System' (2004) 47(3) Perspectives in Biology and Medicine 317, 320ff; Stephen Schiffer, 'A Normative Theory of Meaning' (2002) 65(1) Philosophy and Phenomenological Research 186; Tom Stonier, *Information and Meaning: An Evolutionary Perspective* (Springer 1997) 38, 120.

[51] Paul Horwich, 'A Use Theory of Meaning' (2004) 68(2) Philosophy and Phenomenological Research 351; Ludwig Wittgenstein, *Philosophical Investigations* (3rd edn, Basil Blackwell 1967) 3, 20, 80; Donald Davidson, 'Belief and the Basis of Meaning' (1974) 27(3-4) Synthese 309, 311ff.

[52] Uhlan von Slagle, *Language, Thought and Perception: A Proposed Theory of Meaning* (De Gruyter 1974) 25, 37-38.