Pontifícia Universidade Católica
do Rio de Janeiro

Thallita Gabriele Lopes Lima

Better justice through better science-technology? The entanglements of algorithms and security and legal professionals

Tese de Doutorado

Thesis presented to the Programa de Pós-graduação em Relações Internacionais of PUC-Rio in partial fulfillment of the requirements for the degree of Doutora em Relações Internacionais.

Advisor: Profª. Drª. Isabel Rocha de Siqueira

Co-Advisor: Profª. Drª. Manuela Trindade Viana

Rio de Janeiro

August, 2024

Pontifícia Universidade Católica
do Rio de Janeiro

Thallita Gabriele Lopes Lima

Better justice through better science-technology? The entanglements of algorithms and security and legal professionals

Thesis presented to the Programa de Pós-graduação em Relações Internacionais of PUC-Rio in partial fulfillment of the requirements for the degree of Doutora em Relações Internacionais. Approved by the Examination Committee:

Prof. Isabel Rocha de Siqueira
Advisor
Instituto de Relações Internacionais, PUC-Rio

Prof. Manuela Trindade Viana
Co-Advisor
Departamento de Relaciones Internacionales
Pontificia Universidad Javeriana

Prof. Fernanda Glória Bruno
Programa de Pós-Graduação em Comunicação e Cultura, UFRJ

Prof. Rodrigo José Firmino
Programa de Pós-Graduação em Gestão Urbana, PUC-PR

Prof. Alcides Eduardo dos Reis Peron
Instituto de Relações Internacionais, USP

Prof. Luísa Cruz Lobato
Instituto de Relações Internacionais, PUC-Rio

Rio de Janeiro, 02th, August, 2024

Thallita Gabriele Lopes Lima

Graduated in International Relations at the Federal Rural University of Rio de Janeiro in 2016 and obtained her M.Sc. Degree in International Relations from the Pontifical Catholic University of Rio de Janeiro in 2020.

Bibliographic data

Lima, Thallita Gabriele Lopes

Better justice through better science-technology?: the entanglements of algorithms and security and legal professionals / Thallita Gabriele Lopes Lima ; advisors: Isabel Rocha de Siqueira, Manuela Trindade Viana. – 2024.
256 f. : il. color. ; 30 cm

Tese (doutorado)–Pontifícia Universidade Católica do Rio de Janeiro, Instituto de Relações Internacionais, 2024.
Inclui bibliografia

1. Relações Internacionais – Teses. 2. Algoritmos. 3. Segurança. 4. Reconhecimento facial. 5. Erros. 6. Clearview AI. I. Siqueira, Isabel Rocha de. II. Viana, Manuela Trindade. III. Pontifícia Universidade Católica do Rio de Janeiro. Instituto de Relações Internacionais. IV. Título.

CDD: 327

To José, Átila, Thalles, and Wesley for their unconditional support, affection, and love.

Acknowledgements

This thesis is, above all, an entangled. Different times, spaces, people, and things made it possible, and it would take another volume of similar size to thank everyone who made it happen. Anticipating the partiality of the result and exercising, once again, an old passion of mine for impossible causes, I will try in the following lines to mention and acknowledge some of those who, perhaps without knowing it, brought this study into being.

To my grandparents Glória, Sebastião (*in memoriam*), Júlia and José. They had no access to formal education, but from them I learned about the vastness of the worlds that exist. I want to thank my parents, José and Átila, for their affection, encouragement, and understanding, for being deprived of my company many times, and above all, for supporting my choices. They have always believed in education as a path, and even if I can write here in English, it is because of them. Thank you for everything you have done for me. To my brother Thalles, for taking me in and bringing me lightness and laughter in tense moments and for looking after me from the start. My family was the best witness to my co-transformation, with whom I practiced patience and through whom I learned more about myself, love, and dedication.

To my life partner, Wesley, who would deserve many chapters of thanks. Your intelligence, unrestricted support, non-negotiable values, affection, and unique way of being poetry and a safe haven have written this work with me. Thank you for your infinite patience in my tense moments, for your constant willingness to help, for always being there for me, and for sharing all your anxieties, doubts, dreams, and experiments with me. You always calmed me down, which was fundamental for me to overcome the difficulties along the way. It is an immense joy to share a planet, a time, and a life with you.

I would like to express my sincere gratitude to the National Council for Scientific and Technological Development (CNPq) for their financial support through the Doctoral Scholarship. This support has been instrumental in enabling my research and academic development. This study was partly financed by the Coordination for the Improvement of Higher Education Personnel - Brazil (CAPES) - Finance Code 001. This support was fundamental in enabling me to

dedicate the time and resources needed for this study. The infrastructure and resources provided were essential to the progress of my research.

I also like to express my gratitude to the Institute of International Relations professors and staff at PUC-Rio. Special thanks go to two people who inspired me as a researcher, teacher, and human being, as well as sharing the path that made this research possible. Firstly, my advisor Prof. Isabel Rocha de Siqueira's comments, conversations, advice, attention, and affection were essential for this work and beyond. I would also like to thank Prof. Manuela Trindade Viana for her willingness to be my co-supervisor and for her willingness to listen to me. I can safely say that your participation was central to this work, and without you, my reflections would not have been the same. Isabel and Manuela, thank you for making this journey intellectually stimulating, challenging, and highly enriching.

To the members of the qualification committee, Dr. Daniel Edler and Prof. Anna Leander, whose suggestions and criticisms during the qualification were fundamental to improving this work. I thank them for their intellectual generosity and commitment to my academic development. Indeed, to the members of the defense committee, Prof Fernanda Bruno, Prof. Rodrigo Firmino, Prof. Luísa Lobato, Prof. Alcides Peron, and Prof. Maíra Siman, for agreeing to participate in the process of finalizing this research and whose valuable contributions will help to refine the arguments and strengthen the conclusions of this thesis.

To my dear colleagues from the class of 2020 for the moments shared. I would like to extend my gratitude to the Surveillance Studies research group at the Vrije Universiteit Brussel. Their welcome and partnership have been instrumental in the development of this work. I want to acknowledge the STS & Feminist, Gender & Sexuality Studies group at Cornell University, whose collaborations and discussions have enriched this space of learning and discovery. I am also grateful to all the interlocutors I met at the international and national events I presented at, whose perspectives and questions were crucial to the evolution of the ideas presented here.

The weaving of this work would not have been the same without my work as a research coordinator on the Panóptico Project. For this reason, special thanks to the Center for Security and Citizenship Studies (CESeC), a fertile space for

learning and producing research with ethics, responsibility, and care. As well as being a place of affection. I would like to thank all my colleagues, especially the Panóptico team for all their listening, partnership, and ability to dream and build collectively. In particular, I thank Pablo for the partnership we have built of complicity and trust. With the challenges, you have given me, "throwing me out of my comfort zone," I have matured as a researcher and person in these years walking with you. Moreover, to my crystals from Baixada Fluminense, Thaís and Rodrigo for their caring gaze, companionship, and fondness.

To my activist colleagues from the #Tiremeurostodasuamira campaign, with whom I learned so much and shared ideas and possibilities for (re)thinking forms of imagination and collective struggle. To colleagues at the ACLU and their generosity in sharing data and experiences. I want to thank the dear journalist Laís Martins for all the conversations and threads we have followed about Clearview AI.

To my dear friends who I have made and who have made me along the way, I will not name them all, but you know who you are. Thank you for understanding my absences, for the visits, for the meetings with laughter and food, for taking care of my plants on my travels, for the memes sent, and for the hugs and tears. You are present in all the senses of the word.

The materialization of this study is mainly due to the support I received from the people who accompanied me along the way. To all of you, my sincerest thanks. Each of you, in your unique way, has been part of this process. This work is a testimony and was only made possible by the human and more-than-human entanglement in weaving its realization.

Abstract

Lima, Thallita Gabriele Lopes; Rocha de Siqueira, Isabel (Advisor) and Viana, Manuela Trindade (Co-Adviser). **Better justice through better science-technology?: the entanglements of algorithms and security and legal professionals.** Rio de Janeiro, 256p. Tese de Doutorado – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

In security, algorithms have become prevalent and used by institutions such as intelligence agencies, police, and courts. These technologies, including facial recognition software, are employed in various security and surveillance practices worldwide. This widespread use raises questions about algorithms' epistemic authority and credibility, particularly in producing (in)security practices and contesting evidence within the criminal justice system. In this context, this thesis explores the complex entanglements of the practices of security and legal professionals and algorithms, emphasizing how these digital technologies materialize, stabilize, and circulate in diverse practices even amid errors and contestations. First, the thesis examines the implications of algorithmic reason, addressing how these technologies simultaneously promise efficiency and objectivity while repeatedly getting it wrong. It then explores how algorithms shape perceptions, identify targets, and influence security actions, focusing primarily on biometric data and facial recognition algorithms, such as the use of Clearview AI in the United States. By analyzing these systems, the research aims to understand how algorithms create and legitimize "better justice/security" imaginaries and their broader social and political consequences. The thesis is located within Critical Security Studies, Science and Technology Studies, and feminist critiques of technoscience, crossing different fields to understand the operative characteristic of algorithmic reason in international politics. Finally, the research demonstrates how algorithms create conditions of possibility for security and justice practices, organizing a multitude of elements and producing an order that impacts these fields and highlights the importance of understanding the political force of the discourses surrounding algorithms and their role in reformulating the conditions of possibility for thinking and doing security.

Keywords

Algorithms; security; facial recognition; errors; Clearview AI

Resumo

Lima, Thallita Gabriele Lopes; Rocha de Siqueira, Isabel (Orientadora) e Viana, Manuela Trindade (Co-Orientadora). **Melhor justiça através de melhor ciência e tecnologia? Os emaranhados de algoritmos e profissionais segurança e direito**. Rio de Janeiro, 256p. Tese de Doutorado – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

Na segurança e Justiça Criminal, os algoritmos tornaram-se prevalentes, utilizados por instituições como agências de inteligência, polícia e tribunais. Essas tecnologias, incluindo software de reconhecimento facial, são empregadas em várias práticas de segurança e vigilância em todo o mundo. Esse uso generalizado levanta questões sobre a autoridade epistêmica e a credibilidade dos algoritmos, particularmente na produção de práticas de (in)segurança e na contestação de evidências dentro do sistema de justiça criminal. Neste contexto, essa tese explora os complexos emaranhados das práticas de profissionais de segurança e do direito e algoritmos, enfatizando como essas tecnologias digitais se materializam, estabilizam e circulam em diversas práticas mesmo em meio a erros e contestações. Primeiro, a tese examina as implicações da razão algorítmica, abordando como essas tecnologias prometem simultaneamente eficiência e objetividade, enquanto recorrentemente erram. Seguidamente, explora como os algoritmos moldam percepções, identificam alvos e influenciam ações de segurança, focando especialmente em dados biométricos e algoritmos de reconhecimento facial, como o uso Clearview AI nos Estados Unidos. Ao analisar esses sistemas, a pesquisa visa entender como os algoritmos criam e legitimam imaginários de "melhor justiça/segurança" e suas consequências sociais e políticas mais amplas. A tese se situa dentro dos Estudos Críticos de Segurança, Estudos de Ciência e Tecnologia e críticas feministas da tecnociência, compondo com diferentes campos para entender a característica operativa da razão algorítmica na política internacional. Por fim, a pesquisa demonstra como os algoritmos criam condições de possibilidade para práticas de segurança e justiça, organizando uma multitude de elementos e produzindo uma ordem que impacta esses campos e destaca a importância de entender a força política dos discursos em torno dos algoritmos e seu papel na reformulação das condições de possibilidade para pensar e fazer segurança.

Palavras-chave

Algoritmos; segurança; reconhecimento facial; erros; Clearview AI

Table of Contents

List of figures

It matters what matters we use to think other matters with; it matters what stories we tell to tell other stories with; it matters what knots knot knots, what thoughts think thoughts, what descriptions describe descriptions, what ties tie ties. It matters what stories make worlds; what worlds make stories.

Danna Haraway, 2016, p.12.

Part I

Algorithm, biometric data and security practices

1.
Introduction

This dissertation is about how entanglements of (in)security are made possible, materialize, stabilize, and circulate by and through security practices with and through algorithms, even amid errors, failures, and contestations. The last decade has witnessed a significant increase in the presence of algorithms in different dimensions of international politics and our daily lives. Apparently, they are everywhere. Algorithms are circulating in many spheres and places around the world: they can decide a remote target in wars using drones, whether or not we can access public services, whether we get a job interview, how much credit we can access, and what news we can see in our social media feed. These dynamic computational systems (GILESPIE, 2014) shape digital knowledge and sociability and impact our socio-material[1] relationships regarding how we recognize others and are perceived. More and more states and societies are beginning to understand their problems through the lens of algorithms. One example is that governments use them to make impactful decisions about our lives, from the health benefits we can receive to whether or not we will be charged with a crime.

Algorithms are multiple and dispersed. The term 'algorithm' has become a buzzword in contemporary governance practices, but its meaning is unclear. In the strict sense of the term, an algorithm is the description of a finite and unambiguous sequence of steps (or instructions) to produce results (output) from data (input). For example, a cake recipe is an algorithm, as one can be made from its ingredients. For a computer to execute an algorithm, it must be written in a computer language and coded into a program (a kind of text that includes written instructions, also known as "source code"). This program can then be run in software or compiled as an application. In this strict sense, algorithms can be understood as a sequence of instructions for a computer to implement an activity on data.

As we have seen, algorithms are increasingly becoming objects of concern and debate, not only in the technical sphere and computing and engineering, but also in other academic fields and civil society. We often come across the term even

[1] Sociomateriality in this thesis emphasizes the distribution of action and agency emerging from practices enacted by both humans and non-humans (MOL, 2002).

in our informal conversations about the recommendations of social networks and streaming apps. According to Seaver (2019, p. 412), as more and more aspects of our social lives are conducted alongside and through algorithms, both online and offline, people who once had little interest in the workings of algorithms are increasingly concerned about their effects. This concern has manifested itself in an explosion of popular and academic productions that engage with algorithms in terms that bear no resemblance to the more technical concept of what an algorithm is (SEAVER, 2019).

Algorithms comprise much more than code: they need instructions on expectations, standards, and risk limits; technical platforms that make data mobile; and interfaces to enable access, use, and functionality (DE GOEDE; BELLANOVA; 2022). In addition, they link society, technology, and nature in a mesh of relationships. Moreover, they work through multiple operations of relating things: in the many practices of relating, building, tinkering, and applying that, algorithms gain their power to reshape and order different things. In this dissertation, the idea of algorithms is mobilized not only as well-defined sequential steps to generate an output, but also as a political proposition about the world and the conditions of possibility for thinking about it (AMOORE, 2020; 2022; ARADAU; BLANKE, 2022).

Under these terms, algorithms function as a way of gathering and ordering knowledge that also profoundly transforms how societies understand themselves. According to Amoore (2022), algorithms have changed the political technologies of governance of international politics. However, they themselves are reordering the conditions of possibility of what politics itself 'can be'. There is a vast interdisciplinary literature, with many contributions from the field of International Relations, which proposes to study the effects of the use of these technologies in different social and political dimensions (AMOORE, 2020, 2019; ARADAU; BLANKE, 2018; AUSTIN; BELLANOVA; KAUFMANN, 2019; DE GOEDE, 2020).

In similar lines of ambition, this dissertation engages with Critical Security Studies, Science and Technology Studies, and the feminist critique of technoscience, aiming to understand how algorithmic reason is an operative feature of international politics. It is because this rationality(ies) creates conditions of

possibility for a way of thinking and doing security and "better justice" (but not only) that it orders and organizes a multitude of things, individuals, practices, and discourses, producing an order. Therefore, the contribution of this dissertation to the study of international relations lies in the consideration of technology, especially machine learning algorithms[2], in the composition, circulation, and stabilization of security practices and in how order is (re)produced through these technologies.

In the practices of security agencies and the criminal justice apparatus, the presence of algorithms has also been pervasive. Indeed, several security institutions have used these computer technologies: intelligence agencies, as revealed by the Snowden documents in 2013[3]; the police, in the case of crime prediction software (such as PredPol, HunchLab, Precobs and Maprevelation) and facial recognition software (Clearview AI and Rekognition, for example); criminal courts, which have used DNA forensic statistics algorithms; and parole boards, whose decisions increasingly depend on risk analysis algorithms (such as the Correctional Offender Management Profile for Alternative Sanctions – COMPAS). At least 75 of the 176 countries around the world actively use algorithmic technologies for security and surveillance purposes. These include smart city/safe city platforms (56 countries), facial recognition systems (64 countries) and smart policing (52 countries) (FELDSTEIN, 2019).

It is worth noting that algorithms are, in fact, just one of several digital technologies that are reshaping the categories and practices of the penal apparatus and the ways in which these practices can be challenged. In this sense, here I delve into the depth and complexity of how the epistemic authority and credibility of the algorithm produces conditions of possibility for practices of (in)security. With this move, my goal is to understand how these technologies have been affecting the

[2] Machine Learning is a technology in which computers can learn according to expected answers through associations of different data, such as images, numbers, and anything that this technology can identify. Machine Learning algorithms are created from the data that will be analyzed. The answers (or results) at the end of the analysis process offer the system ways to learn and reincorporate for further analysis. The system can generate its own rules or questions to be answered through probabilistic inference (SVENSÉN; BISHOP, 2011). After training, the machine learning algorithms can be used in real-time analysis to learn on their own from the data (HOSCH, 2020). Through this experimental process based on trained data, the algorithm automatically and gradually improves itself.

[3] See also the European Court of Human Rights judgment in Zakharov v. Russia in 2015, no. 47143/06.

possibilities of contesting evidence as it traverses the practices of criminal practitioners.

This introductory chapter aims to provide the reader with a framework for following the path proposed by the chapters of this dissertation and is divided into four sections: (1) the presentation of the puzzle that the dissertation proposes to analyze; (2) the conceptual framework and methodological composition; (3) the presentation of the research strategies and methods used; and (4) the overview of the chapters.

1.1. The Puzzle: the trouble and the promise of algorithms

We live in a time of problems and promises arising from advances in science and technology, especially in what is understood as Artificial Intelligence (AI). Historically situated conditions have enabled security practices to emerge and spread through digital technologies. In the broader social discussion about framing the security problem and its solution, algorithmic technologies are one piece of the puzzle. For Jasanoff and Kim (2009), security technologies and social developments condition each other in a "co-evolutionary" process that prevents the identification of simple cause-and-effect relationships. What we do and what we think co-evolve together (HAYLES, 2006, p.164). Machine learning algorithms frame modes of perception/representation and, as such, how they constitute/condition the solutions and responses we can give to certain phenomena.

Often discursively framed as more objective, faster, and more precise than human analysis and decision-making, algorithmic governance and management practices have been presented as a more efficient, objective, and reliable option for states interested in saving costs and increasing the speed of bureaucratic and other procedures. It should be noted that the construction of objective knowledge and objectivity is not independent of the cultural and bureaucratic practices surrounding it (DASTON; GALISON, 2021; HACKING, 2006).

As we will see, many benefits are associated with using digital technologies, including speed and efficiency in data analysis. The possibility of analyzing large volumes of data has become central to the "big data era," marked by a widespread belief that the more data, the greater the intelligence (BOYD; CRAWFORD, 2012, p.663). Algorithms, especially machine learning algorithms, have been seen as a

solution to latent security issues to deal efficiently with possible dangerous futures (terrorism, crime, disorder, and migration issues, among others.). The large volume of data allows a wealth of inferences through correlations and an equal number of potentially justifying factors for speculative security actions and decisions (FERGUSON, 2016; DE GOEDE, 2012).

In another discursive key, digital technologies have also been presented as a solution to so-called "racial bias" and to abuses of various kinds committed by the police. In 2011, the National Institute of Justice (NIST), the research, development, and evaluation agency of the US Department of Justice, published the article "Police Science: Toward a New Paradigm." The document calls for a "radical reform of the role of science in policing"; this reform prioritizes evidence-based policies and actions and the need for more intense collaboration between universities and police departments (WANG, 2019). Key points in the discourse supporting the use of algorithms are those of efficiency, precision, and scientific rationality.

Here, there is a frequent discourse that algorithms will vaporize biases and heuristics inherent in human judgment and reasoning – which, in turn, would increase the legitimacy of security and justice agencies and confine the application of punishment to the "pure" scientific method and "reason." The reformulation of police practice towards evidence-based scientific methods, for example, would shift the growing criticism between police officers and the arbitrary use of force, penal selectivity, and discretionary power (WEISBURD; NEYROUD, 2011), in addition to conferring greater investigative efficiency and the ability to prevent violent events, such as terrorism. According to Ferguson (2017, p.29), the adoption of algorithmic and data analysis strategies arose from a need to "turn the page" on scandals that revealed systemic problems with policing tactics – especially concerning racial and geographical profiling – and the penal apparatus as a whole.

The problems related to this “page-turned” expectation placed on algorithms have been widely discussed not only by civil society organizations, but also by academics, journalists, and public managers (EUBANKS, 2018; O'NEIL, 2016; BROWNE, 2018; ANGWIN et al., 2016). One of the axes of this debate concerns the exposure of the race, gender, and nationality biases with which algorithmic technologies operate in security practices. For some organizations, the use of these technologies in both policing and criminal justice negatively affects the

due process, a fundamental pillar for guaranteeing rights in legal systems, such as the presumption of innocence and the right to a fair trial – the right to understand what they are accused of and the evidence against them.

For the European Union Agency for Fundamental Rights, discrimination in decision-making based on algorithmic data analysis is "a fundamental area particularly affected by technological development."[4] Reacting to concerns raised about algorithmic bias, the Council of Europe's European Commission for the Efficiency of Justice adopted a "European Charter on the Use of AI in Judicial Systems"[5] in 2018 in an attempt to mitigate the aforementioned risks, specifically in the justice sector. Despite the various criticisms addressed to the use of these systems, computer scientists, technology providers and policymakers insist that algorithms not only improve the efficiency of justice, but ultimately make the criminal justice system fairer (SIEGEL, 2018).

The work of agencies like the Commission mentioned above reveals a concern to reduce risks and harm as far as possible or even a belief that it is possible to rectify algorithms to make them more objective and less harmful to the guarantee of rights. Acknowledging problems but pointing to ways of rectifying or mitigating harmful effects, these discursive practices end up reinforcing the value of algorithms in terms of efficiency and objectivity: to the problems arising from algorithms, the algorithm itself is offered as a solution – but an improved version of it (AMOORE, 2020). Despite the political importance of exposing the inefficiencies and biases of algorithms – despite a discourse that promotes them as efficient and objective formulas for dealing with a large volume of data and misconduct – this research will follow a different interpretative approach.

More precisely, I want to explore the effects of the growing use of algorithms by instances of the penal apparatus not despite the discourse of efficiency and objectivity, but as implications that are authorized and made legitimate precisely because of the political force of this discourse. To this end, it

[4] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. Fundamental Rights Report 2018. Available at: <https://fra.europa.eu/en/publication/2018/fundamental-rights-report-2018>. Accessed on: May 15, 2024.
[5] CONSELHO DA EUROPA. Carta Ética Traduzida para Português (Revista). Available at: <https://rm.coe.int/carta-etica-traduzida-para-portugues-revista/168093b7e0>. Accessed on: May 15, 2024.

is essential to understand a set of contributions seeking to reveal the inseparable nature between these technologies and social processes (SEAVER, 2013, p.10). Each result of an algorithmic system depends on a multiplicity of data, human judgments, algorithmic assumptions, limits, and probabilities (AMOORE, 2020; GILLESPIE, 2014). In origin, the algorithm that works in machine learning is not neutral or without bias because it needs assumptions to extract resources from its environment to adapt, learn, adjust, and adhere.

The question is not whether the tendency to use algorithms to resolve uncertainties in security and legal practices is good or bad but to reflect on what this algorithmic way of thinking and doing makes possible. As noted, algorithms have been understood as a solution to security problems by extending cognition and analysis beyond the human. In this way, algorithms implement pre-established security visions and "abductively generate" threats and targets by recognizing patterns[6] in large volumes of data (AMOORE; RALEY, 2017, p.6). There is a growing discourse based on the belief that the constant optimization of algorithmic provisions is reliable enough to deal with security problems efficiently.

The construction and stabilization of trust in algorithms is this research's focal point of interest precisely because it reveals the regime of truth constituted through these technological resources. The proposal is to offer a situated explanation of how algorithms build credibility, especially those that use biometric data such as facial recognition. The discourse of "perfectibility" (ROCHA DE SIQUEIRA, 2016, p.2) is central to this discussion, as it reveals a central aspect of the discursive authority invested in algorithmic processes, namely the understanding that the "errors" pointed out in a given algorithm are part of the process of perfecting it. It is a deviation from the expectation that the algorithm will make 'perfect' calculations and from calculating and learning the algorithm. In machine learning, the process is uninterrupted because its error does not appear as a breakdown but as a potential for optimizing the existing system.

As algorithms become increasingly pervasive in providing solutions for decision-making from risk management to the criminal justice system, they hold

[6] A pattern is a grouping of data (an entity, an event, an object) as a simple definition that can take on a label. And it's the way algorithms recognize when something or someone is a threat, a security risk (LEESE, 2014).

out the promise of a particular truth claim. The particular mode of truth-telling of machine learning algorithms refers to "ground truth": a labeled set of training data from which the algorithm generates its world model (AMOORE, 2020, p.136). Machine learning algorithms increasingly derive their own "ground truths" from raw, unclassified data, so the algorithm generates what is anomalous or normal in the data. This technology traces problems and solutions through parameters that it learns when exposed to the data, and the algorithm's way of stating the truth is commonly considered an optimized output.

Thus, in this thesis, I explore how this reliability attributed to algorithmic processes impacts the production of a regime of truth, with effects on the rationality of "evidence" with which the penal apparatus has historically operated. More specifically, the research will analyze the effects of the discursive authority attributed to algorithms in their growing use by police, intelligence, and criminal justice professionals, especially when forming evidence that guides operations (stop-and-frisks and arrests) and judicial proceedings. With this in mind, I seek to address the following research question: how does algorithmic reason circulate and affect the possibilities of contesting evidence when it crosses the practices of criminal justice professionals? Here, I seek to explore three major concerns:

a) How do algorithms recognize and make perceptible to the analyst what a "target" is? What conditions do they offer for security action?

b) What are the effects of the entanglement between algorithmic reason and legal and security professionals, especially when it spills over into spaces such as the courts?

c) What does this tell us about normalizing a way of showing and telling a true story that is difficult to dispute based on algorithmic results?

Driven by these concerns, I examine closely and literally follow the development, technical functioning, and entanglement of machine learning algorithms with professional security and legal practices. In this sense, the idea is to "analyze algorithms in situ" (AMOORE; PIOTUKH, 2016, p.13) and observe the socio-legal processes and infrastructures that make possible the rationality(ies) with which algorithms operate. Despite a growing ecosystem of algorithms used in the criminal justice system, this research will be interested in security practices using

biometric data, specifically facial recognition algorithms that have gained adherence, expanded, adapted, and circulated as a security practice in different countries.

As we have seen, facial recognition algorithms are widely used to reinforce, support, and/or improve security practices. They are part of a broad set of technologies that range from the already established process of collecting and analyzing fingerprints to police management software and crime "prediction." For this reason, after diving into a broad analysis of the use of algorithms in security practices, this dissertation will have as its nodal point the intersection of the use of biometric data and facial recognition algorithms. To this end, the research is composed of an analysis of Clearview AI's facial recognition algorithm, which expresses the attempt to reflect on how algorithms have created conditions of possibility for specific forms of perception (for example, how to make evidence visible beyond the possibility of human observation), identification and recognition (who is or is not recognized) and what this produces when added to the practices of security and legal professionals.

The analysis of Clearview AI helped me to understand both the performative[7] layer of the algorithm and the discourse of efficiency and optimization that authenticates the credibility of its practices (understanding how these specific systems are reliable even amid criticism, controversy, and errors), as well as allowing me to observe how particular security practices are enacted in other spaces, such as in courts. In this investigation, I have taken into account the diversity of actors in each specific space of experimentation, seeking to reinvigorate this diversity in a sense that is attentive to the effects of errors and biases in producing differential modes of distributing security, but understanding that it is not up to us here to think about how these effects can be avoided or anticipated by a given set of norms.

As we noted above, the demands for reform of the police and the penal apparatus more broadly have intersected with technological advances, especially

[7] The concept of performativity, which forms the basis of this project, is derived from the works of Mol (2002) and Barad (2007). According to these authors, performativity suggests that the ontologies of bodies and phenomena are not pre-determined and fixed, but are continually produced through knowledge practices. This understanding of performativity is crucial to our analysis of Clearview AI and its impact on security and legal practices.

machine learning algorithms capable of making valuable propositions: the results are not falsifiable, but the correlations of the attributes are ‘good enough’ and can be recombined – therein lies their usefulness. It could mean new, less discriminatory security, legal practices, and/or the optimized reflection of the same practices. This "new paradigm" is not merely a reformulation of the models and practices used by law enforcement but a revision of the image of the police and the criminal justice system[8]. The attraction of algorithms depends on their ability to fill a configuration to reshape and execute things in new ways through the rendering[9] and optimization of practices (RUPPERT, 2013). The narrative of technocratic domination of innovative practices can bypass central political questions about interests and alternatives and replace them with references to technology as a 'better solution.' According to Wilcox (2016, p.16), subordinating the world “to its impersonal logic and the reign of calculability and instrumental rationality.”

Algorithms relate to and order a multitude of things (for example, different types of data, materials, methods, times, places, and social relations), with sometimes unpredictable consequences in the creation and legitimization of imaginaries of what this 'better justice/security' would be. I recognize here the particular risk of adopting the word “justice” in this dissertation. Justice is a powerful rhetoric that is difficult to resist and can produce obstinate activism and a loss of criticality (ROSE, 2004). These problems are exacerbated when justice is coupled with the universalisms of science (JASANOFF, 2005; 2006). Much suffering has been wrought by hegemonic and colonial efforts to construct science and justice together; a single form of knowledge and a single justice excludes many others. Therefore, disturbing ideas of technoscientific justice and development help us to moderate any tendency towards a prefigured universalism of what justice

[8] In an article for Scientific American entitled "How to Fight Bias with Predictive Policing," Eric Siegel (2018) describes predictive policing as "an unprecedented opportunity for racial justice" and the ideal platform on which new practices for equity can be systematically and widely deployed. The New York Times article "Even Imperfect Algorithms Can Improve the Criminal Justice System" (2017) reaches similar conclusions. While the article's authors acknowledge the need to check and balance algorithmic systems to avoid disparate outcomes, they conclude that "well-designed algorithms can counter the biases and inconsistencies of humans and help ensure equitable outcomes for all."

[9] Rendering is the processing and combination of digitized raw material such as images, videos and audios and the resources incorporated into the algorithm. This process transforms one or more files into a single output, unifying these elements with the aim of optimizing analysis and user experience.

looks like. Instead, I try to remain modest and work to be attentive to the specificities of each situation (HARAWAY; GOODEVE, 2015).

Thus, this dissertation is an invitation to (re)think what counts and is framed as algorithmic 'error' and 'failure.' That is why I accepted Haraway's (2016) onto-political invitation to "stay with the trouble" in his words,

> [s]taying with the trouble does not require such a relationship to times called the future. In fact, staying with the trouble requires learning to be truly present, not as a vanishing pivot between awful or endemic pasts and apocalyptic or salvific futures, but as mortal critters entwined in myriad unfinished configurations of places, times, matters, meanings (HARAWAY, 2016, p.1).

The insistence on the problem operates as a precondition for practicing critique without denunciation (AUSTIN, BELLANOVA; KAUFMANN, 2019), avoiding possible traps that bring dichotomies that fail to account for the complexity of the algorithm and the broader architecture in which it is inserted while working with and within these often problematic, diffuse and confusing socio-technical systems (KAUFMANN; LEANDER; THYLSTRUP, 2020). The idea is to reflect on how our perspective is recursively linked to how algorithms "know" and "do" (AMOORE, 2019). Thus, this research intends to strange existing normalities and technologies (FOUCAULT, 1989), to turn the surface and dive into the multiple practices and entanglements that, at least for now, make algorithmic evidence in the practices of both security and criminal justice professionals, possible.

We should remember that the successful production of a given reality is always a realization, which depends on power contestations, polemics, and the credibility gathered (ARADAU; HUYSMANS, 2019) by those who produce different and often conflicting versions of that reality. The dilemma is not to delineate the good use from the bad use of algorithms but how these technologies can rapidly circulate in various domains of our social life, updating, reshaping, and legitimizing worlds of security.

1.2. Composition and diffractive reading

Diffractive readings bring inventive provocations; it is good to think with them

Barad, 2012, p.3

In this thesis, I set out to "diffractively" read insights from different disciplinary fields, particularly to (re)think about how machine learning algorithms, especially of the facial recognition kind, have become possible in security practices. As Isabelle Stengers (2004, p.15) argues, composing with different elements leads us to think with them, in other words, to think differently. It will be a careful exercise to compose and bring together diverse insights that will allow us to understand how algorithms play a fundamental role in security practice.

A diffractive reading using ideas and concepts from different authors makes it possible to explore ideas productively, paying attention to the gaps in each theory and making it possible to perform new propositions "intra-actively." Barad (2007), via Haraway (1992), suggests diffraction as a methodology and a way of seeing the world. According to Haraway (2004, p.280), diffraction is a "mapping of interference, " not a replication, reflection, or reproduction. A diffractive reading does not map where differences appear but rather "where the effects of difference appear" (HARAWAY, 2004, p.280). Diffraction is about reading insights through each other, understanding the details and specificities of relations of difference and how they matter (BARAD, 2007, p.71), and shifting to questions of practices, doings, and actions.

This approach helps us analyze the various sites, dynamics, and processes through which security and insecurity materialize intra-actively. It also requires a fundamental reconsideration that theories and knowledge production are not mere conceptual tools for studying security but crucial participants in its intra-active materialization and the processes through which (in)security comes to materialize intra-actively in International Relations.

In physics, diffraction refers to the behavior of waves when they encounter an obstacle or a crack; they spread out in various directions instead of following a linear path. Here, I will offer an example of a visual experiment: a CD can be a diffraction apparatus. This object produces and makes visible the different

characteristics of light, which is why we can see the rainbow of colors in Figure 1. Diffraction is a way of creating patterns that show interference and telling us what is being diffracted. In the case of the CD, it is light – so we can say something about the light, or we can say something about the diffraction apparatus (BARAD, 2007, p. 83). Barad (2007) uses this metaphor of diffraction to address how different ideas, theories, or entities interact and influence each other, producing new and often unexpected patterns. In this section, I explore concepts that are essential to this research.

Figure 1. Diffraction of the light

Source: experiment carried out by the author.

‘Materializing’ is a differentiating process in which the differences that come to matter matter in the intra-active production of different differences. The changing patterns of difference are neither pure cause nor pure effect; they produce, or instead promote, a causal structure, differentiating cause and effect (BARAD, 2007, p.137). I believe that Barad's notion of matter, mainly through the concept of "intra-action," manages to make progress towards dispelling the idea of machine learning algorithms separate from the rest of the world. The concept of intra-action offers a mode of enunciation for referring to the processes of producing the world

without resorting to previously established boundaries. One of the main effects of reading Barad is to be wary of establishing boundaries before studying practices. In this sense, in the case of this research, it is a question of thinking about the production of security practices by and through algorithms based on the actions that formulate the very boundaries of what is considered thinking and doing security.

Another concept that is central to this work is that of "apparatus." Like matter, in this reading, apparatuses do not have a fixed exteriority but are contextual stabilizations operated by specific practices. According to the author: "in an agential realist approach, apparatuses are specific material configurations or rather dynamic (re)configurations of the world through which bodies are materialized intra-actively" (BARAD, 2007, p. 169-170). Bohr's concept inspires this concept of apparatus. However, the author criticizes Bohr's proposal because it presupposes the existence of a human observer outside the apparatus. In Barad's version, the apparatus no longer ends in the "human," nor does it have a prior boundary between human and non-human. In the author's approach, the concept of apparatus can even be defined as the "conditions of possibility" for certain phenomena to materialize (BARAD, 2007, p. 143).

In this sense, as Barad notes (2007), these apparatuses do not work "correctly" most of the time. The "interferences" produced by these so-called failures are incorporated by Barad (2007) as an essential part of the apparatus and the production of a phenomenon since it is through these "errors" that those apparatuses are generally perceived. In the concept of apparatus, there is a reformulation of the very idea of "measurement," which is seen by modern science as an objective possibility, that is, without interference (BARAD, 2007, p. 137). For Barad, the "phenomenon" is the very ontological inseparability intra-actively performed by the apparatus. As such, "any measurement of position using this apparatus cannot be attributed to some abstract, independently existing object, but rather to a property of the phenomenon - the inseparability of the object and the measuring agencies" (BARAD, 2007, p. 139).

Under these terms, phenomena are not the mere result of laboratory exercises carried out by human beings. Instead, phenomena are differential patterns of matter ("diffraction patterns") produced through complex agential intra-actions of multiple material-discursive practices or apparatuses, where apparatuses are not

mere instruments of observation but boundary-drawing practices – specific material (re)configurations of the world – that become matter. These casual intra-actions need not involve human beings (BARAD, 2007, p. 140). In this way, given the indeterminate nature of nature itself, intra-actively performed and open to constant (re)figurations, what about the question of objectivity? For Barad, it is precisely the recognition of the (in)determination of phenomena and their inseparability from their measuring apparatuses that guarantees the possibility of thinking about a concept of objectivity. Not one that presupposes the separation of entities, but one that recognizes the existence of an "agential cut" (BARAD, 2007, p. 140) that performs a relationship of contextual causality.

In this sense, the materialization of the algorithm in security practices is, for Barad (2002; 2007), both material and discursive since they consider this division a Western border project. In this line of thinking, being recognized as a possible risk through a facial recognition algorithm means operating an ontological relationship with a perceived, recognized, and classified body. It opens possibilities for thinking about producing dangerous subjects from techno-scientific apparatuses, which occurs through localized and always unstable practices. Thinking about the practices of materializing security through and by algorithms also allows us to map the blurring and contingencies at play in their production.

Barad argues that representationalism is an act of erasing the practices involved in the production of a given fact. The "images or representations are not snapshots or representations of what awaits us, but condensations or traces of multiple practices of engagement" (2003, p. 53). In this sense, this process of erasure operates in scientific practices in such a way as to eliminate the operations through which something is given the status of a ‘fact’.

The emphasis in this reading is not on the possibility of multiple ontologies but on the relative stability conferred on the matter after it has emerged intra-actively due to the same apparatuses producing the same result. Thus, Barad (2007) helps us extend the idea that 'things could be otherwise' into the ontological realm but conceptualizes specific moments in which things are stabilized 'as they are' by understanding processes through which particular properties emerge. Other realities can be excluded from existence through cuts and exclusions. I suggest that there is a radical potential in Barad's perspective, which is to draw attention to what is being

excluded from particular materializations. Compounding this socio-material approach, Hacking (2006) provokes us to reconsider what it means to be invented and produced through the practices of classification and representation by and through algorithms.

In line with what Coleman and Rosenow (2016, p.206) call an "ontological commitment to an unchallenged and privileged notion of security," the proposal in this thesis is to follow machine learning algorithms in practice in a broad social context in order to understand how they play a role in perceiving, recognizing and classifying particular ways of life. According to Hacking (1986, p.166), if new modes of description emerge, new possibilities for action emerge in tandem. The possibility of action, in this sense, is closely linked to the models of perception, recognition, and description of attributes embedded in our everyday practices. Furthermore, it is becoming increasingly urgent how the limits of perception, recognition, and attribution have been drawn in/by machine learning algorithms.

Given the scenario of claiming a foundation of truth in algorithmic analysis that permeates our contemporary imagination, algorithms can close the door to the future (AMOORE, 2019). It is because this imagination that offers algorithms as a "solution" to problems closes the gap in the difficulty of the decision (AMOORE, 2019). The algorithm generates a contingent probability of an absolute decision (for example, guilty or not guilty) and thresholds of normality and anomaly. While the machine learning algorithm works with correlations and probabilities, it also advocates a malleability and management of expectations in action in the present. The science of machine learning algorithms seems to transform the relationship between science, knowledge, and doubt (AMOORE, 2019, p.2). They do not eliminate doubt but incorporate it productively (DE GOEDE, 2012; AMOORE, 2013). Machine reading algorithms are constantly reconfiguring and adapting to respond to their own errors and failures (KRASMANN, 2020).

In this sense, I propose to produce an attentive, plural, and partial investigation into how error is part of the algorithmic learning process and what its acceptance can tell us about the changes in how the security problems posed by and through algorithms are being analyzed. In this sense, in collaboration with various fields, the idea is to think of a way of critiquing algorithmic rationality(ies) in security practices that not only "unmask" errors and manipulations but also looks

at how algorithms create the conditions of possibility for a specific way of doing and thinking about security that is perpetuated and reinforced. This dissertation aims to develop a critique beyond suspicion (AUSTIN, 2019, p.216). It is decidedly less totalizing, modest in its claims, detailed in its analysis, and open to complexity and the diversity of possible interpretations (AUSTIN; BELLANOVA; KAUFMANN, 2019).

1.3. "Following a thread in the dark"

Nothing is connected to everything. Everything is connected to something.

Haraway, 2016

As algorithms have become part of the ecosystem of security technologies, they have also become an object of interest for International Relations (IR) researchers who, over the last two decades, have started to look into various issues, such as the construction of these technologies (AMOORE, 2019; 2020; ARADAU; BLANKE, 2021; 2022), what role they play in the production of these practices and to what extent they can benefit or compromise the security and integrity of marginalized social groups (O'MALLEY, 2017; LEESE, 2014; BELLANOVA; DE GOEDE, 2020; WILCOX, 2016). However, just as tricky as investigating the practical and even ethical issues raised by these technologies in the security field is how to research them. It is precisely this question that this thesis also addresses as it proposes to look at algorithms as a relational and ontologically entangled practical scientific apparatus that does not exist independently of other phenomena and agencies.

Knowledge practices and being are not isolable; they are mutually implicated. Knowledge is not produced because we are outside the world; we know because we are of the world. We are part of the world in its differential becoming. The separation of epistemology from ontology is a reverberation of metaphysics that presupposes an inherent difference between the human and the non-human, subject and object, matter and discourse. So, thinking about 'ontoepistemology' is probably a way of thinking about the kind of understanding we need to agree on the importance of specific intra-actions. (BARAD, 2007, p. 185).

In this sense, it is important for this dissertation to think about the conditions of possibility that have made algorithms practical security solutions. This research advances a view of security as an intensely relational and ontologically entangled phenomenon that does not exist prior to or independently of its intra-action with other phenomena and agencies. Understanding the ontologically entangled nature of security suggests, paraphrasing Barad (2007, p.217), that security "is not a preexisting object of inquiry with inherent properties. Instead, it should be understood as a phenomenon constituted and reconstituted from historically and culturally specific iterative intra-actions".

The analysis proposed in this research will be to trace and map the entangled practices with a focus on the places where this way of doing and thinking about security is being produced and reproduced to understand how this is being done and made possible materially (SUCHMANN, 2002). As we have observed, it is essential to consider the human and non-human agencies involved in this process, observing the expected and unexpected combinations and collaborations, as Haraway (2016, p.3) proposes: "following a thread in the dark." By tracing and pulling the threads that weave this tangle, the aim is to observe the relationships and patterns that are essential to our understanding of these processes in which what the algorithms say is taken as the "truth" (AMOORE, 2020; GILESPIE, 2014).

Researching algorithmic practices requires methodological reflections, especially in contexts where opacity, secrecy and the unknown are constitutive of dominant security practices with and through these technologies (WALTERS, 2015). Rather than silencing the possible challenges that arose when exploring specific security entanglements and machine learning algorithms, I followed the thread in the dark and, through it, questioned overarching political imaginaries. If we focus on unpacking what Huysmans (2011) calls the “little security nothing”, we can understand a broader logic of how these are made possible. The scale, in this sense, can be the result of ongoing mundane processes of production and contestation and reproduction (BARAD, 2007, p.245).

It is worth starting the conversation about methods in the middle. The path to this research began during the global COVID-19 pandemic in 2020. As Deleuze and Guatarri (1995, n.p) contend, "[it is] that the milieu is not average; on the contrary, it is the place where things acquire speed." The global health crisis is

entangled with advances in implementing algorithms and digital technologies in our daily lives. It has shaped the conditions under which the research was conducted and the very configurations of the composition of methods that made it possible for this thesis to materialize. In this context, the choice of analytical strategies was not simply applied, but emerged through continuous engagement with the material-discursive practices in which I was entangled. Inevitably, all the choices made in this disserttaion are about being in the middle of several fronts, and it also highlights that in making choices and drawing boundaries, other dimensions became lateralized. The point is that we cannot simply bracket certain dimensions without taking responsibility for the constitutive effects of these cuts (BARAD, 2007, p.58).

The central ambition evolves from the description and the tracing of the entanglements of algorithmic practices and security and legal professionals even in the "dark thread" or in the uncertainty of where it will lead, and not stop at the difficulties and limits of opacity or secrecy (DE GOEDE; BOSMA; PALLISTER-WILKINS, 2019). Nevertheless, I made the limits my threshold for studying machine learning algorithms and the security and legal practices they enact, without forgetting that algorithms do not emerge or develop and operate in a vacuum but are part of political and social practices that are often confusing and complex. As Introna (2017) points out, to understand algorithmic practices, we do not necessarily need to understand or know the codes but observe them on the surface of the visible: how they do, what they do, and what they make possible. Researching tangles without disentanglement is a persistent challenge (BARAD, 2007) in collecting and analyzing data and writing the thesis. In this sense, I focused on the phenomena and their insistence that they are not only examined by research but constituted by research.

In this way, the indeterminacy of entanglements has led to many difficult questions about what unpacking empirical data is like. Barad (2007) offers an answer that recognizes that phenomena are not simply measured or examined by the apparatus. Theoretical concepts and ideas are considered materially in the apparatus and help to produce and describe what is being observed. In this sense, structuring this dissertation involves reporting and describing data in conjunction with the thinking that helps create the phenomenon.

The thesis dives into the case of Clearview AI, a company that has a facial recognition machine learning algorithm that has been circulating among different security professionals and that fits into a global trend of increasing demand for the (re)use of biometric data for the purposes of producing order (FERGUNSON, 2017; CRAWFORD, 2021; HOFMANN, 2018), sometimes in a way that allows them to circumvent legal safeguards to ‘guarantee security’.

As mentioned above, the research began in 2020 amid what was perceived as the Clearview AI "scandal." In the New York Times article, "The End of Privacy as we know it?" the company, which at the time held 3 billion images collected from open internet data sites, presented a technology that was 'different from all facial recognition algorithms previously used in the United States (HILL, 2020). The debate about Clearview AI highlighted severe privacy and legal concerns associated with using facial recognition technologies and how, even amid error and ethical questions, this technology has expanded into several global markets.

How does the facial recognition algorithm offered by Clearview AI become useful and good enough to guarantee security amid uncertainty? The Clearview AI case was chosen for this thesis in an attempt to reflect on how algorithms have created conditions of possibility for specific forms of perception (for example, how to make evidence visible beyond the possibility of human observation), identification, and recognition (who is or is not recognized) and what this brings out and makes possible when added to the practices of security and legal professionals. The case allowed us to observe how particular practices of (in)security are enacted in other spaces, circulate, and (re)shape themselves, (re)composing and assembling credibility and epistemic authority.

For this analysis, I propose a methodology aimed at exploring the material-discursive entanglements that (re)produce algorithmic reason as sufficiently credible – despite all the criticisms – with attention to the effects of this regime of truth on what is understood as evidence in the field of action of security and legal professionals. Inspired by Barad's (2007) concept of ‘materiality’, the idea is to follow and analyze processes of materialization, the processes by which matter (heterogeneous entities) acquires meaning. Barad (2007) analyses how discourse and matter are co-constitutive: objects do not precede subjects or vice versa; both

emerge as specific types of objects and subjects through processes of materialization.

> Neither discursive practices nor material phenomena are ontologically or epistemologically prior. Neither can be explained in terms of the other. Neither is reducible to the other. Neither has privileged status in determining the other. Neither is articulated or articulable in the absence of the other; matter and meaning are mutually articulated (BARAD, 2007, p. 152)

Analyzing the relationships between algorithms, practices, humans, institutions, and discourses allows for a deeper understanding of the complexity of the processes of writing machine learning algorithms and the security practices they make possible. As Latour (1999, p.188) argues, the results of events are not entirely dependent on human or technological action but on the relationship between them. In this way, by paying attention to how algorithms have agency, for example, in constituting new domains of life as knowable, recognizable, and amenable to intervention, there is no contradiction or exclusion of the importance of discourses in framing certain technologies as reliable and/or objective solutions.

In line with this perspective, algorithms in security practices emerge through discursive particularities and specific material arrangements. To this end, the research will go through, more generally, four confusing methods compositions: (1) analyze the discursive practices; (2) mapping; and (3) tracing and describing. Given the challenge of focusing on various parts, especially when these socio-material agencies are entangled and constantly reshaping and entangling themselves. In short, the proposal is, through mapping, tracing, and analysis, to expose the ambivalences, inconsistencies, and cracks that failures and errors can openly produce in discursive material practices in the materialization of security practices with facial recognition algorithms, but without losing the focus involved in the demarcations necessary to achieve the research and the commitments to the questions proposed by it.

Analyze the discursive practices of the problems for which machine learning algorithms are framed as an optimized security solution. To observe the relationship between problem and solution and what the solution has to say about how the problem is framed. In addition, to track and also discuss the controversies surrounding the use of Clearview AI, I used systematized data from open sources, including media data (e.g., news articles and television documentaries, channel

interviews), Clearview AI company online publications, focus groups, social media, commercial data, technical reports (such as working papers and reports written by think tanks available on the company website), public datasets from journalists and non-profit organizations, and government documents.

Mapping the history of the emergence of biometric technologies and their intertwining with machine learning algorithms as a knowledge apparatus and outlining the speculative field of technical-scientific development they singularize. This mapping is done through a composition of different fields for a comprehensive literature review on both the development of biometric data and the development of algorithmic technologies, especially those that use biometric data such as facial recognition, have materialized as solutions that are good enough to deal with the insecurities of an uncertain scenario. In this mapping, I will do a diffractive reading of the data, which implies reading the data through others and using different literature in conversation.

Tracing and describing the development of a specific facial recognition machine learning algorithm, Clearview AI, from design (technical information, data feeds, training data, among others) to institutionalized use in the practices of law enforcement agencies. I did this by observing the human-algorithm interaction in security practices and its effects on the unequal distribution of (in)security. The choice to dive into just one algorithm is the possibility of a particular access texture and digging deeper into entry points. In addition to the amount of data available on Clearview AI, one example is that much material from interviews, blogs, social networks, patent documents, petitions, open letters, and the company's website offers an important field of exploration for this thesis.

In order to explore what made the implementation and adherence of Clearview AI possible in security institutions and how security professionals use them, I will use the previous mapping of the history of the use of digital technologies in security to carry out a discursive analysis as well as observing in practice how security agents have implemented them. To do this, I collect and systematize data available from open sources. This collection and systematization include media data (e.g., news articles and television documentaries, interviews on channels), online publications, discussion groups, social media, commercial data, technical reports (such as working papers and reports written by think tanks), public

datasets from journalists and non-profit organizations, government documents and corporate publications.

More specifically, I analyze interviews and data received via the Access to Information Act with the discourse of the company's corporate agents (CEO, vendors, and board members) and professionals (users) of these technologies (there are several interviews already produced by news portals and civil society organizations with security professionals who use Clearview AI). The interviews help to understand questions about how security professionals (intelligence agents and police officers) collaborate in algorithmic writing. The attempt is to observe the entanglement of algorithms, data, and security professionals that makes materializing these knowledge apparatuses possible. In the best of worlds, I understand that it would be ideal to do participant observation in one of the "experimentation spaces" (security agencies and courts). However, a viable alternative was to use publicly available materials, recognizing the limitations of this analysis.

I also attended technology fairs such as Latin American Security and Defense Exhibition (LAAD) and International Security Conference (ISC) Brazil. Participating in industrial and regulatory academic conferences, such as those offered by the Institute of Electrical and Electronic Engineers (IEEE), was a rich source of information on how the algorithm and its meanings vary. Arguments, technical visions, and pragmatic bricolage were found on mailing lists, patent applications, and GitHub forums. For example, at trade fairs, there is a solid discursive appeal to how quickly and accurately the algorithm does its "job"; you can try it out and see "the magic" happen. At conferences on NIST evaluations, it is possible to observe the discourse of "adequacy" and precision, a form of evaluation where there is technical detail and a more formal discussion. Moreover, in the forums, especially on Github, there are discussions about " demystifying" the Clearview AI algorithm and pointing out inconsistencies in the algorithm's practice. These forums are spaces for socializing developers' knowledge and ideas (it is important to note that the algorithm's code is protected by corporate secrecy, so discussions in forums like Github are limited).

As I have previously claimed, this dissertation also aims to describe and entangle the practices of security and legal professionals with algorithms and what

they make possible. To do that, I will also pull the thread and analyze judicial processes and criteria for the admissibility of evidence produced from technical-scientific methods. Here, I explore academic and technical literature that already discusses the use of digital technologies, especially facial recognition in the courts. Furthermore, I want to show, analyze, and tell stories, cases, and legal processes related to security agencies' use of facial recognition algorithms, specifically looking at the North American jurisdiction where Clearview AI has operated most urgently. I will use data from open sources and interviews that have been conducted and made public.

Bringing up the stories helps us understand how algorithms materialize ways of thinking and doing security and what kinds of rights violations and violence they make possible. Machine reading algorithms bring something to action: surveillance, mobility restriction measures, psychological violence, and even imprisonment. Furthermore, it helps us to understand how, amid accusations of discretion, errors, and biases in these practices - authorized and legitimized within a particular mode of knowledge production that entangles distributed authorship between algorithms and humans - algorithmic rationality is considered a reliable and even "fair" mode.

Finally, according to Rancière (2009), the method can be seen as a built path and not as an a priori path that is followed. The methods of this research were developed and composed in close relation to the theoretical approaches, epistemological positions, and empirical issues specific to the phenomenon I set out to analyze. Understanding a particular phenomenon is not a priori; no previously decided line demarcates the subject (researcher) and the object; it has to do with the research process. The attempt to describe and show relationships and how they stabilize. How can we think about security as a phenomenon that can materialize in different ways with and through algorithms, and what kinds of work and effects do these technologies make possible?

1.4. Mirror of the Chapters

The thesis will be divided into six chapters, including the introduction (the presentation and framing of the puzzle that the research proposes, the analytical

tools, and the structure of the chapters) and one with the conclusions found in the study.

It should be pointed out that the first pronounced effect of paying attention to the specificity of entanglements is that this dissertation cannot simply discuss the dimension of composition in just one section on the conceptual-theoretical framework. The second effect, perhaps more apparent once involved in the writing, is that entangled phenomena are difficult to define in paragraphs and chapters. A related issue is the need to resolve the indeterminacy of entanglements and make a viable cut somewhere.

I describe writing provisionally as respecting commitments to socio-material entanglements while bringing coherence and a suitable form of order to the thesis. The thesis has discrete sections in the first chapter focused on theory and methodology, but the writing of these sections and several others weaves connections between them all. These entanglements are more than signposts back and forth to highlight previous and future discussions. Instead, for example, the theory is discussed through Barad's (2007, p. 396) "fabric of ethicality" approach. Also, it includes methodological writing to account for the notion that ideas matter and that selecting specific foci for attention is an inevitably ethical practice.

Chapter 2, **Blurring chance and certainty through probability and correlations: machine learning algorithms as security solutions**, aims to map the emergence and historical development of machine learning algorithms and how they have constituted themselves as an apparatus of knowledge, a lens for understanding the world. Moreover, analyzing a set of discursive-material forces may be necessary for the analysis of processes of materialization of a socio-technical imaginary of the algorithm as an optimized path to problem solving that contributes to the trust and authority placed in them. In general, I will analyze the specific conditions of possibility under which the particular discourse of algorithms as a solution circulates in practices that become "stable" and dominant for solving security problems, especially in the penal apparatus more broadly.

Chapter 3, **From ‘bio’ to ‘metrics’: how do machine learning algorithms and biometric data produce reliable evidence?** I will initially analyze the intertwining of the history of the development of biometric technologies and

machine learning algorithms with practices of "anomaly" recognition and classification. It is fundamental to understanding the basis of the development of biometric technology automated by algorithms that we will analyze, including facial recognition. It also situates facial recognition algorithms in a long-standing context of calculative technologies made available to the state to deal with the disorder. Next, we will reflect on the reliability of the algorithmic processing of biometric data and the development and circulation of automated facial recognition technologies (FRT).

Chapter 4, **Clearview AI: "Building a secure world one face at a time"**, the proposal is to turn over the surface that has already been drawn in the previous chapter and make a deeper dive into the multiple practices and human-algorithms entanglements that, at least for now, make the evidence produced by the possible in Criminal Justice. In this sense, the idea is to trace the patterns and relationships that may be indispensable to our understanding of the conditions of possibility of the process that makes the story these algorithms tell "truth" and what makes these two algorithms credible or targets of suspicion.

In Chapter 5**, What algorithmic evidence makes possible: algorithmic errors and failures in "practice",** the idea is to analyze from the empirical undertaking made in the previous chapters how the admissibility of algorithmic evidence revolves around trust in these processes. In addition to observing how flexible the idea of reliability can be. How algorithms and laws receive meaning and practical reach and how discourses and algorithmic rationality are represented and contested in (legal) practice. I will seek to explore how algorithmic rationality affects the possibilities of contesting evidence as it traverses the practices of penal practitioners.

2.
Blurring chance and certainty through probability and correlations: machine learning algorithms as security solutions

Over the past 40 years, computational algorithms have begun to appear in almost every area of contemporary life. From the advent of personal computers in the 1980s, the creation of the commercial Internet in the 1990s, and the subsequent emergence of cloud data storage to the continuing advances in artificial intelligence enabled by the application of machine learning techniques (particularly those applied to large data sets), and contemporary environments have become increasingly digitized. Since then, several machine learning algorithms developed in company and university labs have come into our daily practical use. Unsurprisingly, algorithms have also played a central role in many security-related fields, including intelligence, defense, and military policy, foreign security policy (arms control), and homeland security (state security, police, border protection, disaster management, and critical infrastructure protection). Unlike the analogical forms of statistical knowledge developed historically in Western societies, actionable knowledge extracted from a mass of data promises to reveal unexpected insights, refine the predictive analysis, and identify patterns. The machine learning algorithms provide a generalizable view and a technocratic method that reduces profound social issues to produce optimizable and efficient responses.

In general, computational algorithms are designed to collect, process, and exploit the vast trails of data people leave on sensors and digital devices, turning data (input) into manageable outputs that can predict, optimize, and manage security practices. However, it is essential to understand how the algorithms and the security practices in which they operate circulate among geographically dispersed security professionals and produce shared understandings of machine learning algorithms as a solution to our contemporary security issues. In a world where data trails and analyses of human life patterns are thought to produce new forms of knowledge and enable the detection of future threats, machine learning algorithms enable a renewed potential for ensuring security. This is so because, they

operate with chances and certainties blurred through probability and correlations to provide a security decision in the uncertainty.

The general purpose of this chapter is to unpack the machine learning algorithm and to track the emergence and historical development of these technologies in order to understand their encounter and affinities with security practices. More specifically, my goal is to analyze how machine learning algorithms learn and produce knowledge through data; and what this way of "thinking" and "doing" makes possible when it becomes an apparatus of knowledge. This apparatus circulates and stabilizes as efficient lenses not only to understand but also to solve our security problems. Besides, I observe how these technology's credibility has crystallized even amid criticism and contestation.

The chapter is divided into four major analytical moves. First, I will unpack how machine learning algorithms *learn* and how they operate partially and experimentally in a tangle of heterogeneous and dispersed human and non-human practices. In the second, I will analyze the conditions of possibility for the circulation of the discourse on algorithms as a solution in security practices amidst possible dangerous and unstable futures. Next, the analysis will be permeated by the discussion of algorithms as apparatuses, a grid of intelligibility of security issues that defines the limits of what matters in a scene. This rationality operates by producing knowledge and intervening in a phenomenon that it observes, contributing to the trust and authority in machine learning algorithms. The question that will permeate the final discussion is: why do we trust algorithms as a form of optimized cognition? As we will observe, these technologies continue to be understood as "good enough" to produce security even amidst criticisms of error, opacity, and bias – not because they are perfect, but because they are useful in producing order amid instability.

2.1 Unpacking the *learning* of machine learning algorithm

On operational grounds, an algorithm is a mechanism for solving complex logical or computational problems and for processing and calculating quantities of data by finite step-by-step procedures according to well-defined rules without specifying how these procedures are executed and implemented in physical machines (CORMEN et al., 2009). In short, algorithms can be understood as a

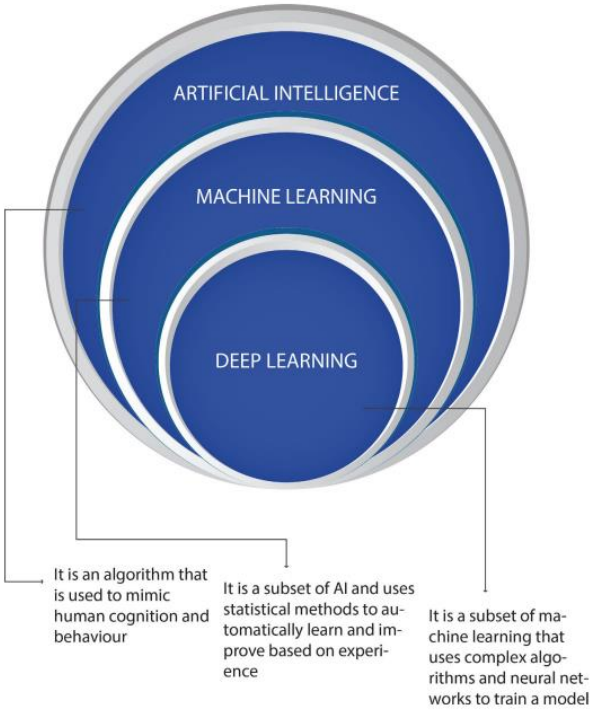
sequence of instructions for a computer to implement an activity based upon data material. According to Tarleton Gillespie (2014, p.1-3), algorithms need not be software, in the broad sense: they are coded instructions to transform input data into the desired output based on specified computations. In computing, algorithms are studied and designed to make computational procedures more efficient and optimized in order to automate processes.

Speaking of algorithms, what distinguishes today's digital world from the previous programming is the availability of big data and its quality, which has radically changed how algorithms are designed, trained, and executed (AMOORE; PIOTUKH, 2016). Throughout the thesis, I will mainly refer to deep machine-learning algorithms. It is important to point out that I will not always make an explicit distinction between supervised learning, where "algorithms learn from a truth model of data labeled by humans" (AMOORE, 2019, p. 5); and unsupervised or deep learning that begins without an initial theory, hypothesis, model, or norm. It is, therefore, essential to understand what we are talking about when we use the terms artificial intelligence, machine learning algorithms (supervised and unsupervised), and deep learning.

Artificial Intelligence is a broad area within Computer Science that generally involves machines that can perform tasks that emulate human intelligence, where the main goal is to perform functions in an optimized and automatic way (CRAWFORD, 2021). It is possible to consider some essential characteristics of these systems, such as the ability to reason[10], learn[11], recognize patterns[12] and inference[13]. Machine learning and deep learning[14] algorithms are a subset of AI, and their goal is to learn from data and be able to predict outcomes when new data is presented or discover hidden patterns in unlabeled data.

Figure 2. Difference between Artificial Intelligence, machine learning and deep learning

[10] To apply logical rules to a set of available data to conclude.
[11] To learn from mistakes and successes so that in the future it can operate more effectively.
[12] To recognize both visual and sensory patterns, as well as patterns of behavior.
[13] The ability to apply reasoning in everyday situations.
[14] Deep learning is one of many approaches towards sophisticated and complex machine learning neural networks that work to train the model algorithm to adapt so that it learns through the volume of data. Deep learning reproduces an aspect of what is understood to occur in human brains, in which there are successive layers of abstraction and, thus, meaning formation.



Source: Elaborated by the author

As more and more aspects of our social lives are conducted alongside and through algorithms, both online and offline, people who once had little interest in how algorithms work have a growing concern about their effects (SEAVER, 2019, p. 412). This concern has been manifested in debates in countless academic fields (Computing, Engineering, Law, Criminology, Social Sciences, just to mention a few), as well as in civil society. Some of these productions have insisted on engaging with algorithms in terms that bear no resemblance to the more technical concept of what an algorithm is (SEAVER, 2019): “a sequence of computational steps that transform the input into the output.” (CORMEN et. al., 2009, p.5).

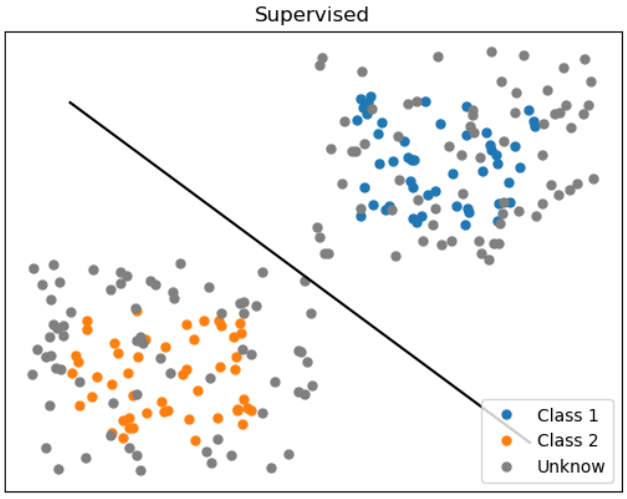
Indeed, the critical algorithm studies literature has been confronting the definition of algorithms in terms of software and code, while insisting that automation must be understood through the various and fluctuating relationships it maintains within the broader social circumstances in which it is situated. In line with these contours, here I will understand algorithm as multiple, entangled, and complex socio-technical systems. The codes with which algorithms operate need instructions about expectations, standards, and risk limits; technical platforms that make data mobile; and interfaces to enable access, use, and functionality (de GOEDE; BELLANOVA; 2022). In this sense, they link society, technology, and

nature in a mesh of relationships. Furthermore, it is through multiple operations of relating things that they work: it is in the many practices of correlating, building, tinkering, and applying that those algorithms gain their power to reshape and order different things. Thus, they are not just well-defined sequential steps to generate an output but also a political proposition about the world and the conditions of possibility for thinking about it (AMOORE, 2020; 2022).

Contemporary complex machine learning goes beyond the programmed 'if, then, else' rules of algorithmic decision procedures based on pre-set rules, seeking instead to generate potential rules and connections from the patterns in the data examples. Here, it is worth reflecting on this distinction between rule-based and unsupervised, deep learning machine learning algorithms. The main difference between these algorithms is the capability to handle unprocessed data and ongoing learning from it. This capability is condition of possibility of the complex and experimental learning arrangement in which algorithms are entanglement with data and human and non-human practices.

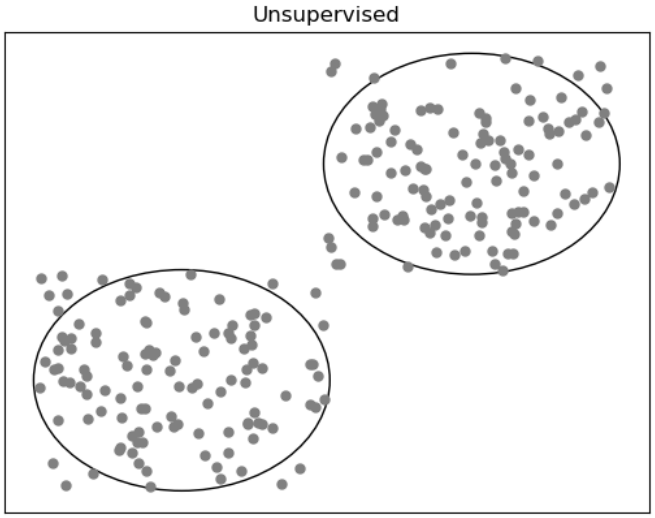
Supervised learning algorithms relate output to input based on data labeled by humans. These data sets are designed to train or "supervise" algorithms to classify data or predict outcomes more accurately. The model can measure its accuracy and learn over time using labeled inputs and outputs. That is, I tell the algorithm the classes I am working with, class 1 (e.g., what is a "dog") and class 2 (e.g., what is a "cat"), and it learns from these predefined labels to identify them, differentiate between them and establish a relationship between them in the data. Unsupervised learning uses machine learning algorithms to analyze and group unlabeled data sets. These algorithms discover hidden patterns in the data without human intervention (so they are "unsupervised"). Unsupervised learning models are used for three main tasks: clustering, association, and dimensionality reduction (making the data manageable).

Figure 3. Supervised Learning



Source: Elaborated by the author

Figure 4. Unsupervised Learning



Source: Elaborated by the author

The defining characteristic of machine learning as a computational method is that it can learn things that exceed explicitly (GOODFELLOW et al., 2016). It means that machine learning, even supervised machine learning, is a generative process that creates knowledge from the patterns and functions available in the data. Machine learning algorithms are, therefore, mainly defined by their iterative relationships with the "examples" to which they are exposed in a data world: it extracts the associated "features" or attributes from these examples. As we can see in Figure 2, even when the data is unlabeled, the machine learning algorithm can assign labels and classifications through inference. With machine learning algorithms, doubt and the unknown are transformed into a malleable arrangement of weighted probabilities of what might be. According to Amoore (2019, p. 2), the

science of machine learning algorithms seems to transform the relationships between science, knowledge, and doubt, to turn an unlikely and unknown event into an actionable action.

The shift from supervised machine learning to deep machine learning approaches is centered on the ability to process raw data in its raw form and constant learning through the data. According to Le Cun et al. (2015, p.43):

> For decades, building a pattern recognition or machine learning system required careful engineering and considerable domain knowledge. Deep learning methods are multi-level representation learning methods achieved by composing non-linear models that transform the representation at one level into a representation at a higher, somewhat more abstract level. With the composition of enough transformations, very complex functions can be learned. (...) The key aspect of deep learning is that these feature layers are not designed by human engineers: they are learned from data using a general-purpose learning procedure.

In this specific sense, deep learning algorithms are more experimental and open in their computation than previous rule-based forms. Computer scientists directly associate a world of more complex multidimensional questions with being addressed, a greater abundance of available data, and the perceived limitations of human-engineered rule-based algorithms. Here, we begin to see the notion that problems are so complex, so multiple in their dimensions, that it is no longer possible for a human engineer to determine the variables, define the rules, and write the program (AMOORE, 2022). There is a resonance between the idea that complex political problems may exceed conventional bodies of knowledge as traditional statistical and probabilistic epistemes. Moreover, the computational idea is that the features of a machine-learning model should be known in advance. Moreover, the computational idea is that the features of a machine-learning model should be known in advance because they operate experimentally with the data.

This research is interested in machine learning unsupervised, a deep learning (neural network) algorithms, which can work with hundreds or even thousands of different features. These algorithms can process and analyzing massive and complex datasets, and the ability to learn generatively and abductively from the data, including current facial recognition technologies, as Clearview AI. For this reason, they are well suited for a world where vast amounts of heterogeneous digital

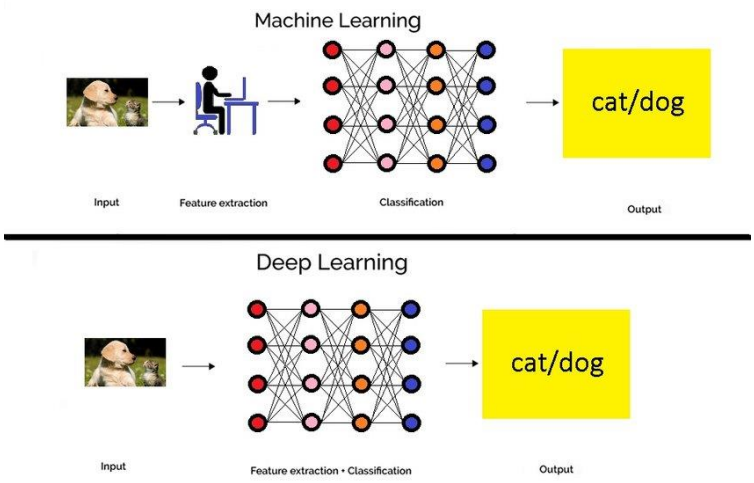
data have become available and increasingly used in contemporary security practices. However, this also means that the scale and complexity of the calculations also mean that the algorithmic decision about which resources are significant is not necessarily reversible to human reasoning. While in some cases it becomes obvious why the algorithm chooses a certain proportion of resources, in other cases, the algorithm's "reasoning" will be opaque and unintelligible to human interpretation. This very opacity is intensified in the case of neural networks.

Neural network algorithms are a modified form of machine learning (see Figure 4) that is becoming increasingly important (MC QUILLIAM, 2018) for developing computer vision algorithms, such as face recognition (VOULODIMOS, et al., 2018; SZELISKI, 2022). They are suitable to forms of input data that are difficult to parameterize and complex to adjust, like the example of faces, which have many different shapes. While humans learn early on to recognize them as they are presented with examples, it is tricky to write a specification that is accurate enough for a machine but flexible enough to handle all possible variations of natural faces. The architectures of neural network algorithms can contain several hidden layers, hundreds of millions of weights, and billions of potential connections between neurons. In the structure of a neural network, there is a set of inputs, called nodes rather than features in this case, and a set of initial parameters intended to map the input nodes onto the target output. The difference is that this mapping goes through an additional hidden layer of nodes (SKYMIND, 2016). Each of the initial nodes is mapped to each of the nodes in the hidden layer, and in turn, the hidden layer is mapped to the destination (the desired outcome classification).

In short, the overall effect can be thought of as the hidden layer allowing the neural network to distill its own feature set, which it uses to discriminate between 'face' and 'non-face,' and 'identified' and 'unidentified,' for example, in face recognition. This way of telling the truth of the algorithm, the decision, is generated from a particular notion of ground of truth in the data (AMOORE, 2019, p.5), that given a large enough training set, the neural network abstracts its own set of hidden features and its ground of truth, which is very effective for complex and multidimensional input data. Importantly, what is implicit in the ground of truth is not what it considers “reality” to be, but the translatability of a problem of interest for which the machine has been calibrated – in the example above: recognizing and

identifying people. There is in this computational process an intensely political process of creation and implementation that implies the distribution of representations in the world in which the algorithm is operationalized in practice. In this sense, understanding how neural networks learn and operate is critical in understanding concerns that these technologies perpetuate gender, racial, or other biases (e.g. BOULAMWINI; GEBRU, 2018). At the same time, any bias can be challenging to identify, explain, and resolve when it comes to how neural networks make decisions. Deep learning algorithms operate generatively in continuous learning cycles, in which their entanglements are reassembled and reorganized experimentally (SEAVER, 2017; THYLSTRUP, et. al., 2022; SUCHMAN, 2007). In this way, we can observe that the opacity of deep machine learning with neural networks is not only that of the black box of algorithms hidden behind the high walls of commercial secrecy: it is also because they tend to be opaque per se and derive their "ground of the truth" from the data (AMOORE. 2020).

Figure 5. How machine learning and deep learning work



Source: Halder et al., 2020, p.2.

In deep learning, as we see in the above image, the final layers are designed to force a result of the nonlinearity of the activations of the points in the data, the nodes, so that the output classifications act as probabilities; that is, they are all values between zero and one and together add up to a total of one (HALDER et al., 2020). The predicted label is the class with the highest probability. Because there is always a 'highest' probability, the option “no probability” cannot be conceived: once processed by the algorithm, something will always be modeled and

categorized. No matter how poor the correlations are, there will always be a predicted output, which explains the certainty that a neural network will choose a result even when presented with deliberately misleading input data.

Algorithms classify by calculating distances, determining an abstract metric of difference as a distance. As illustrated in figures 3 and 4, when data points are closer or further apart, they are assigned different labels. Thus, the foundation of machine learning is 'homophily,' established through the strength of proximity in the data space (CHUN, 2021). This abstract distance in data space is not an inherent affinity but operates on a logic of statistical segregation modulated by the data. Algorithms function as technologies of segregation and ordering, delineating what is essential in a scene (AMOORE, 2020; 2022; CHUN, 2021). In this context, the racial bias in algorithms, heavily criticized by academia and civil society, cannot be entirely mitigated by training with more inclusive data. Algorithmic systems automate discrimination not merely because they are inherently biased, but because their core technical operations involve segregating and sorting based on data experimentation (CHUN, 2021). It is crucial to emphasize that algorithms often learn from decontextualized data, produced and collected in diverse and dispersed ways.

As we have noticed, it is important to develop a greater understanding of how knowledge is assembled in algorithmic systems, including the production of data points due to sometimes complicated and messy socio-technical networks. It also brings up the work required in managing digital data, which is never "raw" (GITELMAN; JACKSON, 2013). They must be "collected, prepared for the algorithm, and sometimes excluded or downgraded" before feeding the algorithm (GILLESPIE, 2014, p.169). Furthermore, it involves tensions around "language, categorizations, update frequency [and] value granularity," among other issues (PELIZZA, 2016, p.39). Thus, in this research, data structuring refers to the practices that organize and transport datasets, selecting and preparing them for algorithmic processing and the "social processes" that facilitate the acquisition and movement of datasets (GOFFEY, 2008, p.18 -19). Therefore, it is of crucial importance to unveil the power relations underpinning the workflow of algorithmic systems, by critically interrogating the formalizations, encodings, and scripts that allow their learning process to appear as a continuous flow, despite its inherent

adherence, errors, and contestations. Doing so helps us to understand how machine learning algorithms have come to be perceived as an efficient and credibility-stabilizing solution. If, as Latour (2022, p. 802) argues, "smooth continuity is the hardest thing to achieve", then it is critical to explore the conditions allowing for *continuity* to be associated with algorithmic systems despite the several pauses and eliminations of traces of hesitation constituting their learning process.

As noted above, the production of data is an important part of the algorithmic analysis process. Machine learning algorithms do not aim to reveal causal mechanisms: they simply relate the pattern of past observations to the prediction of future observations. Although it does not present logical causes and explanations, it increasingly becomes a justification for action in our daily lives. It behooves us to ask: how does a technology that simply reveals one among many possibilities of ordering patterns becomes so influential in terms of decision-making authority? According to Mcquilliam (2019), a possible answer may be an idea of "viewer consciousness," the understanding that algorithms would be outside the reality they observe and analyze, “therefore” neutral. In addition to that, there is the argument of ontological superiority of algorithms, given their capacity to ‘see’ beyond the threshold of possibility and the granularity of human vision and processing associations from an enormous amount of data available.

These computational systems purport to discern an objective reality as they operate from probabilities of what might be. However, they operate through forms of mathematical and computational objectivity. Algorithms combine dualistic metaphysics that places them as ‘outside’ of the reality it analyzes, a process which results in the production of a seemingly neutral and external authority with a tendency to encourage disregard for the point at which its calculations are applied. It encourages the scientific perspective that Donna Haraway (1988) calls the "view from nowhere": the objective, neutral view that is, by its very definition above, outside of and not localized, simultaneously.

In addition, it contains the abstraction and mathematical reasoning that has historically been mobilized in the creation of evidence. Ian Hacking (2014, p. 84) argues that people have been drawn to mathematics mainly because "they have experienced mathematics and found the passage strange." That experience, primarily, has been the experience of proof: proof that hits us with the inevitability

of its conclusions, making obvious what was previously unknown. This kind of proof is so different from other forms of rationality because it seems to bypass empirical work by producing new knowledge directly from the mind itself based on mathematical logic and deduction (HACKING, 2014). However, although it uses axioms and specific procedures derived from the logical and deductive traditions of mathematics, algorithms operate according to a different set of epistemological standards and produce different experiences of truth.

The goal of the experimental algorithmic arrangement is decidedly not the demonstration of logical deduction from axioms and the production of theoretical explanations; but solving problems in practice, whether through classification, clustering, time series prediction, or network visualization. While such forms of reasoning can and sometimes do figure in discussions about developing new algorithmic approaches to class problems, they ultimately play second fiddle to an altogether more pragmatic logic of feasibility, practicality, and efficiency (LOWRIE, 2017). According to Lowrie (2017, p.12), efficiency is the epistemological code through which data science produces knowledge about algorithms because algorithms "always," address a world of practical tasks for which the technology was developed.

Thus, the evaluation of the machine learning algorithm is not just the performance of the computational substrate (the technique) but the entire socio-technical system within which the algorithmic ensemble operates. As such, unlike proof and refutation in mathematics, discussions of algorithm efficiency are interested in the specific domains operated by algorithmic sets. That is, whether or not the algorithms work; and whether they contribute by generating *actions* to "solve" the problems for which they were calibrated. In the end, it is not about perfect precision and techniques but *how* the algorithms are good enough, for example, to recognize a security threat (this argument will be elaborated further in section 2.3).

In this sense, the power of algorithms comes from the ability to make valuable inferences, abstractions, and experiments with vast patterns and even larger data sets that generate an optimal action. For example, predicting the likelihood of someone doing a specific action, such as an email exchange, may involve hundreds of correlated features (a browsing history of hundreds of URLs,

the browser used, the user's location, time of day, weather conditions, and others). Machine learning algorithms allow us to see connections that were previously invisible. Nevertheless, the very largeness of big data introduces an inherent opacity: even in the simplest algorithms, it is impossible to directly apprehend how it traversed the data because of the number of variables involved and the complexity of the algorithm's function derived from mapping inputs to output. We cannot see how it works; we just have to recognize that it has produced some probability statement about a future state.

The patterns detected by machine learning generally provide "answers" to confusing, contingent, and open-ended questions. These answers do not reveal causes or offer explanations of why and how. By grouping, classifying, and predicting human behavior and action, these systems impose order, balance, and stability on the active, fluid, chaotic, and unpredictable nature of human behavior and the social world in general. These processes are installing a normative, algorithmic view that defines what counts as an anomaly and obfuscates the logic that determines what counts as abnormal (see FOUCAULT, 2009; AMOORE, 2019; 2020). In the algorithmic context, “anomaly” is understood differently from statistical abnormality: rather than articulating a social norm or standard to which regulation aspires, "anomaly detection" emerges procedurally from "the existence of variation in the data" (ARADAU; BLANKE, 2018, p.12).

Unlike statistics, algorithmic operations thrive on the multiplication and proliferation of the tangible manifestations of individual cases. Algorithms include individual differences and characteristics and the relationship between individuals (ARADAU; BLANKE, 2022). Therefore, as Aradau and Blanke (2022) demonstrate, algorithmic reason can seem politically appealing because it transcends the binary individuals/populations of the small granular mass of data, composing with minor details and decomposing the largest multiplicities. One example, which will be explored further in the next chapter, is facial recognition, which targets everyone in a crowd to find the one who stands out as a suspect. The facial recognition algorithm can only know what a "suspect" looks like by comparing it to everyone else and producing modulations of the norm and regularity.

Moreover, there is an "ontological politics" of the algorithm, to use Mol's (2002) terms, that has to do with orientations, how problems are problematized and gain circulation, how bodies are shaped and oriented in specific ways and not in others, and how some things become more or less likely. The power and politics of algorithms may not necessarily be located in the algorithms. However, the most powerful dimensions of algorithms have to do with how these systems govern the possible field of action of others, also how possibilities become more or less available or unavailable to particular actors in particular contexts.

Algorithms make the mass of available aggregate data analyzable in an interactive and experimental process in which humans, data, and machines generate norms and anomalies. In doing so, these technologies, in a sense, decide what matters amidst occlusions-they produce boundaries-they impose their version of reality, a condition of intelligibility of the world (BARAD, 2007), of patterns and probabilities derived from data. By drawing the lines between what counts and what does not, algorithmic analysis can normalize certain behaviors, appearances, and codes of social conduct. In this sense, what matters is not the context of the aggregate data that the norms and anomalies belong to but the ability to level and narrow the field of view to generate an output that can be actioned as an optimal path to issue resolution (AMOORE, 2020, p.43).

The language of anomaly detection has been an increasing focus of machine learning algorithms to capture a change in statistical techniques of fitting observation to moduli distributions of the normal. In this sense, algorithmic computational techniques for anomaly detection differ from traditional statistical techniques for anomaly exclusion. The anomaly does not simply blur the boundaries between normality and abnormality. Instead, it introduces a different logic of calculating regularity based on the normal curve but on similarity and dissimilarity calculations. For statisticians, outliers defy the distribution of normality and abnormality and should be eliminated as errors or noise.

Currently, the anomaly does not simply blur the boundaries between normality and abnormality; it introduces a different logic to the uniqueness calculation that is not simply based on the curve-normal but on similarity and dissimilarity calculations. As Aradau and Blanke (2018) argue, anomalies have become particularly desirable for security professionals in the task of capturing

unknown unknowns, as the documents released by Snowden showed. Thus, contemporary algorithms seem to break with the statistical logic of the normal distribution to find new ways to amplify emergent properties in the ‘tail’ of the normality curve. In this sense, anomaly detection with machine learning algorithms holds new promise for security professionals.

The algorithmic mode of analysis seems to break with the ontological plane of human experiences undergirded by a regime of experimentation on digital data that does not represent an individualized, single object or subject, but a set of emerging relationships between data points. As noted in this section, machine learning algorithms learn to recognize environmental features through their exposure to variability and contingency in experimentation on the data. I have drawn attention to the centrality of "learning" as a malleable conceptual framework that bends according to various practices and grounds of truth in formalizing specific processes intended for algorithmic analysis and decision. Moreover, this process of learning from unknown volatilities is actively enhanced by the fracturing and granularity of social relations and the increased datification of all aspects of our lives. With the increasing complexity of the tasks to which machine learning has been applied over the past six decades, however, agreement on what constitutes the ground of truth that is appropriately stable for algorithmic systems has become exponentially more complex.

A widespread critical response to the complexity has been to understand machine learning algorithms technically through the idea of opening the "black box," a term used to describe their opaque and unknown latent operations (SEAVER, 2017). Alternatively, if we are unpacking machine learning algorithms and understanding them as techno-scientific knowledge apparatuses, we must understand them as a broader entanglement. These technologies not only abstract and simulate social relations but also imbues human cognitions, data, and structures into entangled processes that produce a reality. They are not only a grid for the intelligibility of phenomena but also part of the phenomena they observe: a performative representation practice (BARAD, 2007, p.232). In this way, we can come to a different black box configuration and some different conclusions about how we can think and question machine learning algorithms and the security practices that have been mobilizing such technologies.

Indeed, this question of *how* machine learning algorithms operate directs attention to their epistemological foundations, but also an ontological question of *what* emerges from this analysis. What is a machine trying to learn? What have machine learning algorithms been learning as a security problem? What does “anomaly” stand for? This "what" is implied in a ground truth and, therefore, it is not necessarily a representation of "reality" but rather a translation of a problem of interest, which allows it to be readable and expressed in machine-coded language. As I will analyze in the following sections, the problem that an algorithm is designed to solve in the security domain is not pre-existent to the algorithm functioning: it is produced in broad arrangements of experimental material-discursive practices that circulate and frame machine learning as a good enough solution by what it can make a target actionable for the production of security in a world of uncertainty.

2.2. The needle and the tangled haystack: algorithms and machine learning as solutions to uncertainties in security

> *No comfortable historical reference captures the impact of artificial intelligence (AI) on national security. AI is not a single technology breakthrough, like a bat-wing stealth bomber. The race for AI supremacy is not like the space race to the moon. AI is not even comparable to a general-purpose technology like electricity. However, what Thomas Edison said of electricity encapsulates the AI future: “It is a field of fields … it holds the secrets which will reorganize the life of the world.*
>
> Final Report by USA National Commission on Artificial Intelligence (2021, p.7).[15]

Since World War II, partially autonomous and intelligent systems[16] have been used in security practices. However, the advances in artificial intelligence, with the development of complex machine learning algorithms and the enormous amount of data available, represent a turning point in using technologies in security

[15] NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE (NSCAI). Final Report. Available on: https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf. Accessed on: July 2022.

[16] The term "autonomous and intelligent systems" follows the practice of the Institute of Electrical and Electronics Engineers. The sense conveyed is that of augmenting human capabilities, not emulating them, i.e., it is different from artificial intelligence.

automation. The Final Report by the USA National Commission on Artificial Intelligence (NSCAI) claims that there is no point of return: AI tools are essential to address contemporary security issues. According to the NSCAI, AI is "changing the world," predicting that AI technologies "will be a source of enormous power for the companies and countries that use them." A Belfer Center for Science and International Affairs report, commissioned by the Intelligence Advanced Research Projects Activity (IARPA)[17], determined that AI has the potential to be a transformative security technology due to its ability to drive military and information superiority.

This idea that AI is foundational to optimizing contemporary security practices has been seen in the publications of national AI development strategies in over thirty countries and the regional drafting of a strategy for the European Union. In 2017, Vladimir Putin declared that "whoever becomes the leader in [artificial intelligence] will become the ruler of the world."[18] That same year, the People's Republic of China declared that it intends to lead the world in AI by 2030[19]. Likewise, the United States has made AI and national security a bipartisan priority, by establishing the NSCAI, launching the National Artificial Intelligence Initiative, and creating significant AI efforts in the Department of Defense and the intelligence community. Given this context, where artificial intelligence tools such as machine learning algorithms are increasingly taking the center stage and reframing practices, it is crucial to understand how they have come to be understood as inevitable solutions to security problems.

Modern security history intertwines mathematical sciences, methods, and computing technologies. The most notable technological advances in modern computing were driven by code-breaking efforts and ballistic calculations before, during, and after World War II. Initially, 'computers' referred to people, often women[20], who performed complex computations. This work combined human and non-human resources, paving the way for the development of algorithmic

[17]Available on:https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf . Accessed on July, 2022.
[18] Available on: https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world . Accessed on October, 2022.
[19] Available on: https://www.nature.com/articles/d41586-019-02360-7 . Accessed on October, 2022.
[20] Available on: https://www.washingtonpost.com/outlook/the-brilliance-of-the-women-code-breakers-of-world-war-ii/2017/10/06/ec64ca8a-9e2c-11e7-9c8d-cf053ff30921_story.html . Accessed on October, 2022.

computing. Digital data was only progressively developed as actionable (i.e. computable elements) and storable (thus reusable), as well as computational outputs. Thus, the history of computing not only retraces the abstract models through which computer designers imagine the world and its politics: it also highlights the material practices through which computers relate to and, therefore, generatively act on the world and politics.

The period between 1940 and 1960 was strongly marked by the conjunction of technological developments (of which World War II was an accelerator) and the desire to understand how to reconcile the workings of machines and organic beings. From the beginning of World War II, cryptography became central, with Alan Turing and John Von Neumann becoming the principal cryptanalysts at the British Government's School of Codes and Ciphers at Bletchley Park. In the early 1950s, these two researchers transitioned from computers with 19th-century decimal logic (which therefore dealt with values from 0 to 9) to binary logic machines (which are based on Boolean algebra), dealing with more or less essential strings of 0 or 1. The first fully functional electronic computer was the Colossus, used by cryptanalysts at Bletchley Park starting in February 1944, designed to decypher German codes[21]. Turing and Neumann thus formalized the architecture of our modern computers and demonstrated that it was a universal machine capable of executing what is programmed. In addition to this, Turing raised the question of the possible intelligence of a machine for the first time in his famous 1950 paper "Computing Machinery and Intelligence" and described an "imitation game" where a human should be able to distinguish in a teletype dialogue whether he is talking to a man or a machine. Turing's computing machine and output are fundamental to thinking about the development of computing and the idea of artificial intelligence that we have today.

The origin of neural networks, essential to understanding deep machine learning and computer vision, also dates back to the same era. In 1950, the first 'seeing' was manifested by Frank Rosenblatt's Mark 1 Perceptron machine, which physically implemented his perceptron algorithm for image recognition by

[21] Available on: https://plato.stanford.edu/entries/computing-history/#:~:text=In%201936%2C%20at%20Cambridge%20University,symbols%20(Turing%20%5B1936%5D). Accessed on October, 2022.

connecting to a 20 × 20 array of cadmium sulfide photocells to produce a 400-pixel image (ROSENBLATT, 1958). The hope was that neural networks would overcome the limitations of regular programming and mimic the learning of animal brains (GOODFELLOW et al., 2016).

When Alan Turing questioned the possibility of machines "thinking," it awakened science to this possibility: emulating a type of human reasoning. Nevertheless, despite having developed a theory for information architecture and even a sketch about the 31 possibilities of Artificial Intelligence and Frank Rosenblatt's efforts, the hardware technology of the time did not have enough storage capacity and data processing speed. The term "artificial intelligence" officially emerged in 1956 during the Dartmouth Conference among cybernetic[22] research circles. Researchers in this emerging field of science aspired to create a general intelligence (emulating human intelligence) that could be embedded in computers. The latter would extend far beyond a limited number of fields or tasks. Intelligence and military research agencies have been the main drivers of AI research since 1950. As described by science historian Paul Edwards (1996), these agencies actively shaped the emerging field that would come to be known as artificial intelligence already in its early days. For example, the United States Office of Naval Research partially funded the Dartmouth Conference itself. The construction of what we understand today as computer science and artificial intelligence was heavily guided by military support. Also, often military priorities of command, control, automation, and surveillance, long before it became apparent with machine learning algorithms, could be a "practical undertaking at scale" (CRAWFORD, 2021, p.184).

The development of the field of artificial intelligence since the 1950s has not been continuous and linear, however. If the 1980s were a period of optimism, the following decade came to be known as the “AI winter”, with developments running into still inadequate computing power, insipient data infrastructure, and little available data (TOOSI et al., 2021; FLORIDI, 2020). With the advancement of technology, especially regarding storage capacity and data processing,

[22] According to the Oxford dictionary, cybernetics is the science that has for its object the comparative study of the systems and mechanisms of automatic control, regulation, and communication in living things and machines.

investments and research[23] on artificial intelligence were intensified, eventually resulting in machine learning algorithms. The idea of rules that any computer-human or machine could execute – understood as definitive and conclusive algorithmic procedures – rewrote the architectures of postwar social and international orders (DRYER, 2019).

The Cold War context of competition shaped the computerization process during the second half of the 20th century – particularly cybernetics, with the replacement of analog computers with digital ones. Computational logic was an essential component of postwar rationality and rule-based orders precisely because they extended the sequential rules of the algorithm to politics, administration, and decisions. The idea of order and algorithmic 'stability' in a context of profound transformations and uncertainty gave these technologies the promise of dealing with unknown futures in a way that optimizes outcomes through data management and translation. The specific postwar orders of political and computational rules, functions, and variables are relevant to our understanding of the emergence of contemporary machine learning as a "political order" (AMOORE, 2022). As Amoore (2022) argues, the transformation from rule-based algorithms to deep learning models has also been a condition of possibility for the undoing of rule-based social and international orders, from the challenges of Brexit to European Union integration, austerity politics, and digitalization of welfare states. Specially, by introducing new, unpredictable variables.

As we can see, the science of statistical knowledge, probabilistic modeling, data systems, and behavior analysis was deeply embedded in mid-twentieth-century international relations (HAYLES, 1999). This movement began to contest a world of lost, incomplete, and porous information, keeping it "stable" and transforming it into predictive structures. Algorithmic technologies associated with massive data production became a typical response to heterogeneous and persistent global problems (ARADAU; BLANKE, 2022). As Amoore and Raley (2016) state, international relations and security are historically linked to the development of algorithmic forms of computation. Given that "security practice has historically

[23] According to research by Theodora Dryer (2021), since 2008, there has been an exponential increase in research on these technologies, with over 1.3 million articles published on uncertainty management guided by them.

embraced a computational capacity to act decisively and procedurally in the face of radical uncertainty" (AMOORE; RALEY, 2016, p.2). In this way, the machine learning algorithms that have proliferated and circulated in contemporary security practices can be understood as the revival of a long-standing intertwining of security techniques and practices with techno-scientific development and computational processes.

As we have suggested, I can reasonably situate the emergence of algorithms in security within the history of cybernetics. There is little doubt that the post-9/11 world provided the context for much of the research and development of algorithmic forms of security. For example, the work of IBM computer scientist Almaden Rakesh Agrawal pioneered the "ability to find patterns in accumulated data" for commercial retail companies as far back as the 1980s (AMOORE, 2022). Ten years later, these same standard algorithms would become the mainstay of homeland security systems, with Agrawal pointing to "different features" such as "financial backing" and "Islamic leaders" who would be "written into the rules" (cited in AMOORE, 2013, p.43). Today, with the crystallization of ubiquitous use around algorithmic decision systems in security, it is often forgotten that 9/11 played a crucial role in uniting racialized stereotypes and security rules with the mundane possibilities of private company data mining (BENJAMIN, 2019). Without the ability to speculate about possible connections and to write those possibilities into algorithmic rules, the temporalities of preventive security could not have become as profoundly established as they are today (AMOORE, 2022; BENJAMIN, 2019; CRAWFORD, 2021).

Indeed, the anxiety to identify the 'next terrorist attack' as an amorphous and inexhaustible source of dangers has justified and required an equally diverse and ever-expanding set of security practices based on mechanisms that seek to define that future by extrapolating past instances. As Amoore (2013) explains, governance techniques have shifted in the aftermath of 9/11 from a calculative logic to a probabilistic algorithmic one, focused on calculating possible futures. The anxiety generated by the attempt of anticipation gave authority to new calculative techniques to incorporate unexplained contingencies. So, it is because, in the absence of sufficient data, the algorithm is used to "onto-associate logically unknown values" (AMOORE, 2014, p.59). This abstraction involves a continual

disaggregation and re-aggregation of non-causal data, constantly shuffling relationships until a pattern deemed meaningful emerges from that data. The pattern-finding mode of the algorithm facilitates decision-making processes based on what is not possible to explain because it is only claimed as possibly existing.

The algorithms most widely linked to the desire to "connect the dots" across data stocks and act preemptively were of a specific type of rule-based form and statistical regression[24]. The algorithms available for data mining in 2001 were predominantly designed to identify patterns in a volume of transactions so that rules could be generated for the detection of future events (AMOORE, 2022). While such rule-based systems remain extraordinarily important in security practices, the exponential growth in data availability has accelerated the development of other algorithms.

The rise of big data has been accompanied by a new set of promises about maintaining security and order worldwide. This representation of data as synchronous, or 'real-time,' despite its illusory and fragile nature, carries along the imagination of a security horizon that can reject traditional statistical risk criteria (which need a hypothesis), as well as “see” emerging futures from an analysis of big data, thereby detecting new events (RUPERT; ISIN, 2020; ARADAU; BLANKE, 2018). In addition to "connecting the dots," it has increasingly become necessary to find the "needle in the haystack" through heterogeneous data analysis to reduce, tame, and discern the fog of uncertainty about what may constitute a security threat. For security professionals, the "needle in the haystack" metaphor expresses a set of epistemic assumptions of visibility and invisibility involved in the identification of a “threat”.

In this context, software developers and private companies seized the security problems as business opportunities to invent technological solutions to a specific problem: how to extract value from big data (AMOORE, 2013). As data is increasingly central to legitimizing and guiding security practices, there is a growing influence of private companies in producing these practices (DE GOEDE, 2012). Simultaneously, the government's adoption of a new security strategy paves

[24] Regression is a technique for quantifying and inferring the relationship of a dependent variable (response variable) to independent variables (explanatory variables). Regression analysis can be used as a descriptive method of data analysis (e.g., curve fitting) (IZBICKI; dos SANTOS, 2018).

the way for service offerings and the development of public-private technologies and partnerships. An example of the movement of data and metadata extraction from diverse sources and public-private partnerships comes with the Patriot Act in the USA, which authorizes the National Security Agency (NSA) to collect data from private telecommunications companies without the consumer's consent (CRAWFORD, 2021). Analytics firms devise techniques to delve into the ever-developing streams of big data to analyze its importance for their contractors' goals (AMOORE; PIOTUKH, 2016); while designers develop malleable software that finds new purposes as end users apply it to meet different objectives.

The files revealed by Edward Snowden in 2013 highlight how security agencies and private companies collaborate in the process of extracting all possible data to find anomalies, the "the haystack of the needle". The documents reveal that the technologies once available only to intelligence agencies – which were extralegal by design – are now commonly used tools by law enforcement agencies for crime prediction and even migration governance[25] projects. Today, there are a small number of technology companies that deploy machine learning algorithms, provide their necessary infrastructure and access to massive databases on a global scale, and their algorithms are hailed as superior intelligence solutions (CRAWFORD, 2021, p.6).

As we can see in the previous section, just as important as the use of algorithmic technologies is the massive amount of data that these technologies need to operate in an "efficient" and complex manner. While security professionals demand access to ever-increasing amounts of data, the exponential increase in data brings a gap in the human possibility of analysis. Because, it becomes difficult to process too much data to make actions manageable by filtering the mass of collectible data without a technological tool, as machine learning algorithms. Therefore, more than one associative "connect the dots" epistemology, the "needle in a haystack" metaphor captures the epistemic shift toward algorithmic processing of big data away from problems of data size and scale to seeing opportunities in digital data fragments everywhere (ARADAU; BLANKE, 2022, p.22). The small

[25] Available on: https://www.unhcr.org/innovation/how-artificial-intelligence-can-be-used-to-predict-africas-next-migration-crisis/ and https://aiforgood.itu.int/about-ai-for-good/un-ai-actions/unhcr/ . Accessed on October, 2022.

and seemingly trivial details, the details, simultaneously harbor the promise of building granular knowledge of individuals and governing security from unknown dangers. The ‘small analyses’ turn big data into a series of possible chains of associations, while computer scientists talk about the granularity of information and data granules (AMOORE; PIOTUKH, 2015). In a world of data, nothing is too small, trivial, or insignificant.

As Amoore (2014, p.425) argues, one loosens the language of modern probability and assembles a set of combinatorial possibilities in its place. This contemporary rearrangement of combinatorial possibilities in algorithmic methods rewrites the very grammar of calculus. Contemporary calculus is deploying mathematical devices in such a way that no matter whether something can be predicted, it can only be arranged as a calculus – an algorithmic code, a rule of association of plural elements. As a historian of science, Lorraine Daston (1995, p.5) has argued that the mathematics of probability reveals not only a desire for ever greater degrees of precision and objectivity but an "intelligibility of concepts." For the author, the history of mathematical sciences is characterized by a desire to share an intelligible language of always knowing what it means. Following Danton's arguments (1995), it does not matter so much whether the mathematical models that give rise to the algorithms used in security practices have any sense of adequacy in the world; their relevance lies in their ability to organize propositions and establish an algorithmic decision through which data heterogeneity can be processed. Security practices by and through algorithms, do not replace calculative rationalities – as statistics –, but rather utilize a mathematical science that has already wrapped it intuitively and inferentially to its objectivity (AMOORE, 2014, p. 436).

In addition, the migration of data from drives and servers to cloud storage has opened up offshore data production and storage spaces, challenging conventional territorial jurisdictions and contributing to the complexity of machine learning algorithms (AMOORE, 2020). With the complexification of technologies and the improvement of infrastructures, algorithms now can analyze different forms of data (images, text, video, audio) in spatial cloud-based data locations, as is the case with US intelligence agencies in the 'ICITE' cloud system (AMOORE 2016). This transition from rule-based algorithms to generative forms (machine learning and deep learning) has allowed algorithms to learn regularities and patterns from

input data, generating values and weights when parameters are missing or hidden to make predictions and generate new examples. In short, while rule-based algorithms are deterministic, with clearly defined operating criteria, generative machine learning algorithms are probabilistic, with results that change depending on the learning base and experimental use of the data (AMOORE, 2022).

An illustrative and symbolic example of the growing complexity of machine learning algorithms is the victory of AlphaGo (Google's algorithm) over the GO world champion, Lee Sedol, in March 2016. Unlike chess, GO does not allow memorizing many moves the machine could reproduce but instead generates many possible combinations. In the past, programmers had to detail all the instructions for the task to be automated, but machine learning involves presenting the machine with examples of the desired tasks. In this way, humans train the system by providing data from which it can learn. The machine learning algorithm makes its own decisions about which operations to accomplish the task, allowing it to perform much more complex tasks than a conventional algorithm.

Thus, where rule-based algorithmic security would drive actions on all data patterns within the rules, systems based on deep machine learning will find, learn, and generate new rules. As Luciana Parisi (2013, p.2) writes, "it is no accident that the age of the algorithm has also come to be recognized as an age characterized by emergent forms of behavior that are determined by continuous variation and uncertainty." Understood in Parisi's terms, the space of security problem itself – human habitation in relations of continuous variation and uncertainty – actually underwrites the existence of algorithms that derive rules from contingencies (PARISI, 2013, p.2), or even provide the conditions they need to learn.

Notwithstanding rule-based algorithms remain present in security practice, the historical significance of the increased use of generative machine learning algorithms cannot be overstated. In the context of security, abductive[26] and generative processes do not start with a fixed set of criteria for threat or target: rather, they abductively generate threats and targets through pattern recognition in

[26] Abductive logic is a form of logical inference that seeks the most straightforward and probable conclusion from observations. Unlike deductive reasoning, it produces a plausible conclusion but does not definitively verify its fallibility (SOBER, 2018, p.28). Abductive conclusions do not eliminate uncertainty or doubt, which is expressed in terms of fallback, such as "best available" or "most likely."

large volumes of data (AMOORE, 2019; 2020; 2022). This means, for example, that lists of dangerous people, "blacklists," begin to generate an *adaptive list* – where the norm emerges from the data in a mobile, flexible, and unknown way – in real time based on pattern extrapolation (DE GOEDE; SULLIVAN, 2016). In this way, algorithmic practices focused on finding the "needle in the haystack" articulate other anomalies to be attractive for security purposes, which would not be perceived otherwise. This shift from deterministic rule-based systems to more data and outcome-oriented systems is essential to understanding how experimentation is a foundational part of contemporary algorithmic rationalities.

As we can see, the excitement about deep learning algorithms comes from their potential to learn on their own. Instead of requiring painstakingly careful preparation of pre-categorized training data, they can simply be force-fed to learn from a large number of data sets. In this way, algorithms do not simply implement pre-established security views: they generate threats and targets by recognizing patterns from data (AMOORE; RALEY, 2017, p.6). This means that algorithmic security affects what public and private actors perceive as relevant to security. Although security algorithms may not offer clear evidence as to why a particular subject might be suspicious, their ability to process large amounts of data seems to offer a mechanical knowledge that can justify speculative security decisions (DE GOEDE, 2012).

Critical Security Studies have discussed extensively how security systems are directed to action in the future based on algorithmic identification of unexpected correlations (de GOEDE; BELLANOVA; 2022). This is not strictly a "prediction" goal, but as a process of precaution or preemption (ARADAU; VAN MUNSTER, 2007). Preemptive security practices recognize that statistical predictions regarding suspicious behavior and future deviations cannot be reliably calculated. However, these limits of knowledge are leveraged to use speculative inferences and correlations drawn from a mass of data points, to creatively and preemptively identify possible future suspects. This is what Amoore (2014, p.9) called the "politics of possibility," which:

> acts not strictly to prevent the unfolding of a particular course of events based on past data tracked into probable futures, but to

> anticipate an emerging and unfolding event in relation to a series of projected possible futures.

As this literature shows, algorithmic security is not strictly predictive but works through speculative inference to identify potential futures and suspicions. Thus, advances in deep machine learning algorithms are producing new forms of authority and trust, authorizing what or who is brought to the attention of a security analyst and who, in turn, cannot meaningfully access this authorization process. In chapter 3 of this thesis, I will deepen the debate about how algorithms gather credibility and trust, even *despite* all the criticisms and debates that I will introduce in section 2.4.

In these two present sections, we have noted that the increased trust and credibility in algorithms are part of a more general shift toward the complete naturalization of digital technologies as tools and arbiters in various social and institutional practices with the promise of bringing reliability and objectivity in security decision-making amidst uncertainty and the multifaceted contemporary threats (AMOORE, 2013). Here, I move away from considering credibility and trustworthiness as a fixed characteristic of a particular piece of evidence in this case; a machine learning algorithm-and gravitate toward approaching them as something that is enacted (LAW; MOL, 2006). Trust and credibility are not static: they can change over time and need to be developed, and maintained through the discourses and practices of those who operate these technologies. Therefore, this research focuses on the practices through which 'everyone sort of suspends their disbelief' and agrees that an algorithm is trustworthy, despite possible errors and flaws. How do algorithms allow us to think about sufficiently efficient security solutions? How have we relied on these technologies to frame our problems?

Mythic narratives are repeated throughout the history of the development of the idea of artificial intelligence: computational systems are analogous or even superior in speed and efficiency to human reasoning (CRAWFORD, 2021, p.213). Claims about “superhuman” accuracy and perception, combined with the inability to fully explain how these results are produced, form a discourse about AI. The combination of accuracy and unexplained properties results in the creation of myths about the transcendent capabilities of machine learning, mainly when applied in security environments (CAMPOLO; CRAWFORD, 2021, p.10). We can observe a

central tension in this discourse: claims of high accuracy and objectivity of algorithms that are simultaneously beyond human understanding or explanation of their results. As Rouvroy (2016, p.13) notes, faith in the optimizing algorithmic provisions replaces the process of critical evaluation of what is presented as an automated visualization or decision to the analyst. Thus, as the use of algorithms intensifies, so does the popular narrative of the algorithm as a useful, practical, and efficient apparatus in an attempt to maintain order and security. According to Gillespie (2014, p.13), more than mere tools, algorithms are trust stabilizers, practical and symbolic assurances that their assessments and decisions are fair and accurate, free of subjectivity, error, or attempted influence.

Tarleton Gillespie (2014, p.13) warns us that “although algorithms may appear automatic and pristine, this is a carefully crafted fiction”. The underlying visions of the field of artificial intelligence – of which machine learning algorithms are a part – did not arise autonomously but, instead, were constructed from beliefs, perspectives, and the desire to simplify what is complex so that it can be calculated. These imaginaries are historically and culturally situated interpretations of what "automation" is, the capabilities it expresses, and the promises of efficiency it holds, particularly when intertwined with imaginaries of security, as we noted above. Many scholars highlight that the constitutive role of metaphors, myths, and rhetoric in automation anchors the circulation of the algorithms in various spaces and material-discursive practices as a superior form of cognition. The metaphors such as artificial "intelligence" or machine "learning" sustainably guide a social discourse and feed fantasies and future visions in the broader public as well as in expert communities (CAMPOLO; CRAWFORD, 2021; NATALE; BALLATORE, 2017).

The implicit views of the field of artificial intelligence, did not emerge autonomously. The analysis of machine learning algorithm and its institutionalization into the practices of security professionals draws our attention to the nuances brought about by the use of algorithms and the entanglement of security and legal practices, in which technology is only one piece of a giant puzzle. Predictive security practices strategically use the future to circulate the kinds of truths, beliefs, and assertions that would otherwise be difficult to legitimize. In short, it is not just that algorithms are applied as technological solutions to security

problems but that they filter, expand, flatten, reduce, dissipate, and amplify what can be interpreted as a world to be protected. Suppose machine learning algorithms are seen as more "rational" and reliable than a human analyst, able to lead to the best possible solution and decision. In that case, this suggests that they should increasingly be relied upon to make “simple” decisions on criminal justice and security that, otherwise, would be difficult.

Therefore, understanding how algorithmic reasoning operates as a knowledge apparatus is critical. The following section aims to think about how algorithms operate in a specific style of reasoning based on the discussion we have already done about the way of learning and the context of entanglement between them and security practices. The purpose is to analyze the specific conditions of possibility under which algorithmic reason has circulated in practices that become "stable" and dominant in the way of doing and thinking security efficiently contemporaneously.

2.3. Machine learning algorithms "think" and "do": algorithmic reason as knowledge apparatus

> *Knowing is a distributed practice that includes the larger material arrangement. To the extent that humans participate in scientific or other practices of knowing, they do so as part of the larger material configuration of the world and its ongoing open articulation.*
>
> Karen Barad, 2017, p.379.
>
> *Algorithms embody reasoning.*
>
> Katherine Hayles, 2012, p.49.

As we have observed in this chapter so far, algorithms are not only axes under which security practices operate and are legitimized. They are creating conditions of possibility for a specific way of thinking and doing security that has been perpetuated and stabilized. Here, I will understand algorithms as knowledge apparatuses, in Barad's terms (2007). I will use this concept to demonstrate how entities that may seem individual, such as algorithms, actually emerge through and as part of their entangled intra-action in more extensive experimental arrangements (BARAD, 2007). In machine learning, such experimental setups span a spectrum of more-than-human environments that include computer scientists, data,

algorithms, GPUs, human tracks, wires, and servers, and the contexts range from the criminal system to citizen risk scoring in ad tech to health assessments in insurance.

As knowledge apparatuses, the algorithms are a grid of intelligibility of our social and political world that “cuts” through what matter, and this decision-making process operates amidst an interweaving of a multitude of data, algorithms, and humans. As argued in the previous sections, the conditions of the emergence of machine learning also include *learning* what a security problem is, and it is not pre-defined. The algorithm learns through archived data attributes of the population in a constant remodeling and reorganization of the entangled configurations of the deep learning model's parameters. This generative process is interactive and recursive (AMOORE, 2020, p.54), in which there will always be output. in this way, algorithms are becoming part of what we understand as a security "problem" or "target." The political force of algorithmic decisions lies in this threshold of perceptibility and legibility. The reality that these technologies make possible.

If, as Michel Serres (1982, p. 23) wrote, "To decide is to cut," how can we understand this "cutting" of machine learning algorithms and what this delineation of what matters or not produces in terms of security? What impact does the knowledge production of these apparatuses assume in the production and reproduction of different practices of insecurity and violence? Suppose reality, as Barad (1998) argues, is sedimented from making the world intelligible through specific practices, not others. What is the reality that algorithmic discourses and practices make intelligible, and what is occluded from these practices? These are some questions that arise in a context that has been marked by promises that our problems are solvable through the calculated output of algorithmic decision mechanisms.

According to Parisi (2019, p.94), "it is clear today that the automation of automation involves a cultural transformation in the conceptualization of reasoning with and through machine thinking." The author further notes that automation "is not a formal apriori, but corresponds to the conceptual infrastructure of social practices" (PARISI, 2019, p.97). Parisi (2019) shows that new cognitive capabilities emerging with the development of machine learning algorithms diffuse widely,

intertwining with ways of thinking that permeate the social. In addition, the development of these forms of technology is supported by and actively re-engineer a range of social practices that develop in the spaces in which it is incorporated. Thus, the author guides us to a deeper reflection on the material-discursive relations developed so that the technological devices used for security can operate through new technological forms. At the same time, Parisi (2019) draws attention to how security professionals imagine these technologies and the importance of their imaginaries in creating the conditions of possibility for this algorithmic rationality's emergence. However, by framing machine learning algorithms and their form of security automation as performative, current debates also open up for consideration of the broader political effects of integrating these algorithmic rationalities into security. In the same vein, Anne Balsamo (2011, p. 5) writes:

> The invention of new devices, applications, and tools necessarily involves the manifestation of a number of human practices: new languages; new bodily habits; new modes of interactivity; new forms of sociability; new forms of agency; new forms of knowing; new ways of living and dying.

In this sense, we need to be aware of the foundations that organize our worldview and the material-discursive practices that they legitimize, stabilize, and perpetuate. As we noted, in section 2.2, machine-learning algorithms can generate new norms and boundaries of what can be understood as the "good" and "stable" orders in the world (AMOORE, 2020; 2022). That is, it is not just the case that these technologies are providing new tools and modes of classification for governing society. A significant set of epistemic, ontological, and also political transformations take place when societies begin to understand their problems and themselves through the lens of machine learning algorithms. A "machine learning political order" not only changes the political technologies for governing society, but is itself a "reordering of that politics, of what the political can be" (AMOORE, 2022, p.2).

In this way, algorithmic models have become a knowledge apparatus of an "epistemic form of politics" (AMOORE, 2022): a way of gathering and ordering knowledge of society that fundamentally transforms how state and society understand each other. It is therefore essential in this section to dwell on what we understand as algorithmic rationality(ies) and algorithmic reason and how this

"specific style of thought and action"[27] (HACKING, 2012) has crystallized as a practical knowledge apparatus (BARAD, 2007) central in framing security issues.

Given that machine learning algorithms are an epistemic political form in our contemporary world and govern many aspects of security practices and our everyday lives, we must understand how these epistemic politics operates. Therefore, we need to unpack some concepts that are foundational to this research: that of algorithmic rationality(ies) and algorithmic reason, what their specific contours are, and how this "specific style of thought and action" (HACKING, 2012) can also be understood as in reinserting other experiences, such as that of statistics. What are we talking about when we talk about algorithmic rationality(ies)? What kind of knowledge is produced by them? I suggest that understanding the materialization of forms of algorithmic rationality and the algorithmic reason is crucial to understanding the emergence of machine learning algorithms in security practices and the contemporary knowledge economy, more generally.

Philosopher Antoinette Rouvroy (2012) introduced the concept of algorithmic rationality in her work *"The end(s) of critique: data-behaviorism vs. due-process".* She examined the "rationality of algorithmic governmentality" and described it as a form of "data behaviorism" that does not rely on hypotheses (as in traditional statistics) or testing, and does not require knowledge of individual subjects to predict their behavior by state bureaucracies (ROUVROY, 2012; ARADAU; BLANKE, 2022). In other words, knowledge is not produced about the world, but knowledge is discovered directly from the world (ROUVROY; STIEGLER, 2016). In this research, I understand algorithmic rationality as a kind of rationality that makes possible practices of producing datafied individuals through more efficient decision assertion and optimized knowledge through machine learning algorithms (AMOORE, 2022; CRAWFORD, 2021; ARADAU; BLANKE, 2022). In this rationality, algorithms are apparatuses of a specific style of action and thinking that are fundamental for knowing a certain reality, as well as central in the processes of decision-making and management of that same reality.

[27] Hacking (2002, 161-162) introduced the notion of 'styles of scientific reasoning,' coined based on Crombie's (1994) concept of scientific thinking styles. In Scientific Reasoning, besides citing several problems with the word 'style,' Hacking said that he abandoned the phrase 'styles of scientific reasoning' and returned to Crombie's 'styles of scientific thinking' (Hacking 2009, p.19). Hacking (2012) argued that science was a matter of activity and thinking and that he wanted to emphasize action and intervention; he would use the term 'specific thinking and action styles of science.'

It is worth pointing out that a rationality mode implies simultaneously producing knowledge and intervening in a particular problem, phenomenon, or reality (HACKING, 2006; 2012; BARAD, 1998; 2007).

There is public debate about the power of algorithms, both as disruption or rupture and as continuity of previous processes and rationalities (ARADAU; BLANKE, 2022). The proposal of my research is to carry an analysis through a careful analysis of the emergence of these technologies to understand the transformations it brings in security practices and ways of thinking without emphasizing continuity or discontinuity. Therefore, inspired by the work of Aradau and Blanke (2022) and Amoore (2020; 2022), the idea is to use both concepts: *algorithmic rationality(ies)* and *algorithmic reason*. The use of these two analytical tools makes it possible to draw both continuity and discontinuity entanglements in security practices possible by and through machine learning algorithms.

In line with the arguments of Aradau and Blake (2022), I argue that despite being a different rationality, it is not entirely disruptive. As we have noted in sections 2.1 and 2.2, although machine learning algorithms mark some significant discontinuities with traditional statistical imaginaries of state and society, it is only possible through the recognition of how these transformations underpin the deeply uninterrupted continuities of police violence and state abuses of power, inequality, injustice, and discrimination (BENJAMIN, 2019). Therefore, following Foucault (1991, p. 79), the idea is to pay attention to "how forms of rationality are inscribed in practices, and what role they play within these."

Another central aspect is the choice to be made about using rationality in the singular and rationalities, plural. When I refer to rationality in the singular, I generally encompass fundamental aspects that constitute the way machine learning algorithms "think," as we observed in section 2.1, and what constitutes them knowledge apparatuses. However, there are different types of machine learning algorithms and ways they operate according to the problems they are asked to solve. I know that algorithms are multiple. For example, we have those for individual and spatial risk analysis, content management, facial recognition, credit analysis, microtargeting, and probabilistic DNA genotyping analysis, among countless others. Although these are part of the same specific style of thought and action, each has a genealogy of emergence and particular operational and practical rationalities.

Algorithms are not homogeneous, but the particular arrangements that bring algorithmic rationalities together make them temporally highly visible and organized despite having heterogeneous practices. As Amoore (2020, p.64) emphasizes, in every singular action of an algorithmic system lies a multiplicity of human and algorithmic judgments, assumptions, limits, and probabilities.

In an attempt to deal with the dilemma of one or multiple rationalities without falling into generalizations and leaving out the central details of each algorithm, I add the concept of algorithmic *reason* to the discussion. The concept attempts to make sense of the diversity of existing machine learning algorithms and can be used as a prism to understand how the operation of these algorithms is stable and held together despite apparent practical heterogeneity (ARADAU; BLANKE; 2022). According to the authors, algorithmic reason allows multiple rationalities to hold together and proliferate a heterogeneity of dispersed practices. In this way, algorithmic reason emphasizes how a new, ascendant political rationality unites multiple and dispersed human and non-human practices.

The emergence of algorithmic reason and its materialization occurs through apparatuses that are "simultaneously stable and fragile, enduring and emergent" (ARADAU; BLANKE; 2022, p.5). Algorithms operate in a complex, interwoven network of multinational and multilateral tools, infrastructures, power, and labor relations. Take, for example, the facial recognition system used in Bahia, Brazil, launched in 2019. In its pilot project of using facial recognition for public safety, the Bahia government has acquired software systems and infrastructure from the Spanish company Iecisa, in partnership with the Chinese telecommunications giant Huawei (NUNES; LIMA; CRUZ, 2023). These agreements are standard: the systems that enable the machine learning algorithms possible at scale are often hybrid, with infrastructure from China, India, the United States, and elsewhere, with porous borders, different security protocols, and potential data access.

But what makes algorithmic reason a different mode of rationality? What does this way of thinking and doing produce in security practices? If we compare it to human sense-making, algorithms employ a surprisingly different mode of cognition. Even if they can generate rules, "recognize" people and "read" words and sentences, they do not think hermeneutically (ROUVROY, 2012). By bringing disparate parameters together based on similarity and analogy (ARADAU, 2015),

algorithms accumulate their correlates; they work out degrees of similarity and dissimilarity. In algorithm ontology, the mechanism that connects people is the attribute. The sphere of society and social relations, the clusters, are defined by spatial proximities and distances in their attributes. This mode requires a different imagination of the individual and population, a continuous modulation between the mass and the data fragments. For example, the algorithm can interactively move back and forth between truth attributes of a known population (known in terms of quality assignment) and the feature vector of the unknown that has not yet been found.

In short, algorithms do not consciously think and do; if they learn through observation, this is still incomparable to human feeling and sense-making. Their specific style of thought and action may comprise elements of induction and capture, but algorithms lack intuition. Their ways of learning and identifying patterns based on probabilistic similarities are highly formalized. Instead of drawing conclusions from reasoning, developing hypotheses and explanations, or connecting the dots by being affected by specific indicators and signals, these digital technologies read and discover correlations that, for them, reveal the meaning of a phenomenon. Luciana Parisi (2019, p. 111) explains that we can call what algorithms do "hypothesis making." Algorithmic reasoning operates when they learn from incomplete information and through hypothetical and experimental processing. Data can then be traced both retroactively and speculatively, inventing hypotheses that can lead to new rules, axioms, and truths (PARISI, 2019). It is a baseline feature of algorithmic reason. Moreover, it is generative; we have observed some of these outlines in the previous sections.

Thus, it seems that we are facing a form of reason whose objectivity could seem absolute, given that it would be away from all human subjectivity in formulating hypotheses. The norms and rules seem to arise from reality. There is an idea that the data speak for themselves. However, we must remember that this rationality operates through correlations and probabilities; it is still malleable in managing the expectations of action in the present (AMOORE, 2019). Algorithmic reason transforms the relationships between science, knowledge, and doubt (AMOORE, 2019, p.2). They do not eliminate doubt but productively incorporate it (DE GOEDE, 2012; AMOORE, 2013). Doubt is incorporated into the algorithmic

learning process in its relationship with the world of data and becomes a means of learning and making decisions possible under uncertainty. This way of learning need not eliminate doubt, but it becomes a malleable arrangement of weighted probabilities that generate a decision (AMOORE, 2019, p.3). In this way, doubt is the ground of algorithmic computation, a multitude of doubts in the learning model is flexibly condensed to a single output. According to Amoore's argument (2019), this multiplicity in which doubt operates contains an ambivalence that can be an opening for us to think an opening of possibilities.

In addition, algorithms work to identify possible links, correlations, and inferences to produce abductive conclusions that do not eliminate uncertainty or doubt expressed in that the output is the most likely conclusion from the observations, however, without definitively verifying its fallibility. These abductive forms bring a distinct type of casual reasoning, different from deductive reasoning, in which deductions support conclusions so that conclusions must be true given the closest premises to fallible inferences in which the possibility of error remains (AMOORE, 2020, p.48). Error is integral to the mode of truth enunciation pursued by machine learning algorithms, trained in an ethos of constant optimization. As noted, machine learning algorithms modulate, work in degrees of approximation of a function, and thus it is indifferent to the success or failure of the model (AMOORE, 2020), they work pragmatically. This is because the object of evaluation is not just the performance of the computational substrate but the entire socio-technical system within which the algorithmic set is embedded, as presented in the previous sections. In the correlative mode of operation of these technologies, error and fallibility are not conceived as a problem of the model. Instead, they are part of the learning process for model optimization.

Error is intertwined with the production of credibility and the stability of the algorithm's specific style of thought and action since this stability comes from its self-authentication that is hardly refuted by external parameters of truth and falsity (HACKING, 2012, p.605). Error is part of the process and not external to it. Jasanoff (2017) draws our attention to reflect that the accuracy of the technology is not necessarily related to whether it is validated or not; more than having high levels of accuracy (being "perfect"), the technology needs to be sufficiently efficient and useful about the expected results. According to Lowerie (2017), algorithmic

rationality operates in an altogether more pragmatic logic of science; it operates on feasibility, practicality, and usefulness in a computational temporality that can be real-time. The important thing is to produce a practical, efficient, quick output, not a perfect one. Efficiency is the epistemological code. It is because of algorithms direct to a world of operational tasks (LOWERIE, 2017). The more precise knowledge that algorithmic rationalities promise is the decomposition and recomposition of data and its processing through these computational systems (ARADAU; BLANKE, 2022).

The optimal algorithmic decision "is not about precision, but correlation" (CRAWFORD, 2021, p.204). Correlation is sufficient as it allows these technologies to infer trajectories that condense indeterminate points and extract resources from data about a "target of commercial or government opportunity" (AMOORE, 2021, p.43). The belief that algorithmic prediction is sufficiently accurate and useful is fundamentally about reducing the world's complexities to find a noise that makes order out of the mess.

To understand the specifics of algorithmic reasoning, we can think of it in comparison to the rationality on which classical statistics operates (I will draw some comparisons in the course of the section). Whereas statistics, ideally, are deliberately produced by expert design to gather selected data according to predefined rules and assumptions, data can be constantly collected by default with big data and algorithms. The theory seems dispensable (KITCHIN, 2014) in data-driven approaches where the accumulation of large amounts of data (from heterogeneous sources) and generative machine learning algorithms are understood as solutions to improve our understanding of social phenomena and ensure predictability.

Algorithmic decisions and results are created from specific combinations of data representations. Behind the current machine learning boom, there is also the definition of a consistent way to generate data for the world. The amount of data is also essential in understanding the algorithmic reason. Ian Hacking (2015) described the period between 1820 and 1840 as the "avalanche of printed numbers." The author reflected on Michel Foucault's concept of biopolitics, which targeted the population with its own characteristics as an object of government in the 19th century. This invention was related to the development, especially the birth of

statistics as a science, and associated sciences such as demography and data production practices such as the census and administrative records (HACKING, 2015). Hacking (2015, p.280) emphatically characterized this as the period when "the statistical study of populations comes to accumulate gigantic amounts of data." As Hacking was identifying "gigantic amounts of data," a new term was quickly becoming popular, and today it takes on a planetary scale and dimension. What we understand as big data is crucial to understanding the conditions of possibility of the style of thought and action specific to a mode of doing science that introduces new criteria of truth and falsity (HACKING, 2009). Moreover, how algorithmic reason underpins practices that disrupt distinctions between what "works and what does not" (ARADAU; BLANKE, 2022, p.10).

There is a reconfiguration of tensions in knowledge production through the possibility brought about by big data (we noted some in section 2.2). The role that the growing amount of data and the possibility of capturing information, as metadata, takes on is a corpus that guarantees knowledge while it may never be actionable and in a reality that is not concerned with explaining how things come to be, but only with describing what they are. According to Mayer-Schonberg and Cukier (2012, p.665), big data unravel existing epistemologies and methodologies of knowledge production and alters what the authors call the "social epistemology of modernity." We can observe that there is an authority of knowledge production necessary to govern better associated with modern rationality: to know in order to govern (FOCAULT, 2007), and there is also a re-articulation of this authority of knowledge production driven by big data in terms of volume, variety, and velocity. The very expression "big data" can be formulated this way: big data is simply the excess of speed, velocity, amount of data, and complexity that we can no longer understand with our modern rationality, that is, with the rationality that consisted in understanding phenomena by relating them to their causes.

Furthermore, the type of knowledge generated by algorithmic processes – from big amounts of data – is often in rupture with the representational models of knowledge, whose epistemic strength would be the ability to describe or understand a given reality or phenomenon while remaining faithful as possible to some referent. To a centrality of inductive inference, an open-ended hypothesis is based on available data rather than the deductive inference that logically follows a premise

(CRAWFORD, 2021). The strength of the performative rationality of algorithms is not in describing or representing, but in generating effects and producing realities.

The algorithm's success as a rational and objective management model and the decision is related to this epistemological displacement consolidated in the second half of the 20th century – more specifically, in the post-Second War and the Cold War. It marks the passage from the Enlightenment model of reason grounded in critical reflexivity to a model of rationality based on algorithmic rules and then on the algorithm's generative and experimental action (as we observed in the previous section). However, this passage is incomplete, and these forms of rationality overlap and coexist.

Thus, big data is essential to understanding how algorithmic reasoning provides an "enhanced knowledge base for managing individuals and populations" (MAYER-SCHONBERGER; CUKIER, 2013, p.18), making it possible to see populations and all their complexity through millions of signals from individual relationships. Big data fulfills the epistemological promise of capturing and storing the social whole. There is this promise of complete analysis, but there is no pre-determined whole other than a totality created based on big data and its formatting. Alternatively, as Aradau (2015, p. 23) puts it, "Big data is the new whole." It means that the suspect eventually arriving at the "visibility surface" (AMOORE; PIOTUKH, 2016, p. 6) is not just found as the famous needle in the haystack. Instead, the suspect becomes visible due to multiple artificial processes: abstracting from the outside world, filtering and feeding data into the system, of machine learning algorithms identifying particular correlations and patterns to define what can be considered suspicious behavior. Algorithms can be creative and successfully reveal certain truths, connections, or patterns that we could never have even guessed. At the same time, they teach us to see things differently so that they can also change our thinking about the social.

There are some epistemological lines emerge with big data. The first is the temporality of producing complex diagnoses, rapid real-time analysis becomes possible. The second emphasizes the volume of data, thus complete access to knowledge about large numbers of individuals. This volume of data about individuals translates into the knowledge of the population at large. The third is its ability to capture granular aspects of people's lives, and can make inferences about

attributes of the specific data subjects (ROUVROY; BERNS, 2015; CRAWFORD, 2021; ARADAU; BLANKE, 2022; AMOORE, 2020). According to Aradau and Blanke (2022), algorithmic reason with big data analytics promises to transcend the methodology and logic of distinguishing between the granular and the massive, part and whole. It unites "varied wills of knowledge," transcending the great divides of natural and social sciences, part and whole, language and action (ARADAU; BLANKE, 2022, p.40-43). Algorithmic reason has drawn the boundaries in verification regimes (new ways of identifying the "anomalous"/"normal") and does so by redesigning the relationships between individuals and populations.

What we are seeing emerge in contemporary algorithmic technoscience is an orientation to "truth-telling" that frames how decisions can be made without room for doubt. By bringing up the discussion of the algorithm as an apparatus, and its discursive framing as an objective resource, in a quest that tries to be as close to it as possible to present the "real" for action based on "certainty." This trajectory is quite peculiar: this search for objectivity and certainty is not necessarily translated into a quest for eradicating uncertainty (the algorithm itself operates on probability) but for an attempt to "neutralize" possible future harm, producing order understood as "optimal" amidst the mess. What matters is that it works (HACKING, 1994). The algorithm is efficient and practical in ordering data, people, experiences, and complex temporalities as frictionless narratives for action in the present. In short, as a particular material-discursive set, machine learning algorithms "act" and "think" in such a way that they can also change the way we think about the world as they "redistribute" the sensible (RANCIÈRE, 2006).

2.3. Assembling the critique: when machine learning algorithms become a problem, what is the solution?

Overall, using algorithms in security practices offers an interesting ambivalent dynamic. On the one hand, algorithms find legitimacy and trust – even enthusiasm – by appealing to their sense of objectivity and efficiency. On the other hand, this objectivity, efficiency, legitimacy, and precision have been the object of several problematizations. This section summarizes the main criticisms addressed to the use of machine learning algorithms in security practices. Although the proposal of the thesis is not to focus on the biases and search for error rectification,

the presentation of these controversies is essential to the construction of the argument that errors are an essential part of algorithmic learning, and reliance on them, I suspect, is not tied to their accuracy. How can we make sense of the production and circulation of security practices based on machine learning algorithms even when these technologies are diagnosed as flawed, inaccurate, and biased?

As seen in the previous sections, there is a promise of incredible speed, accuracy, effectiveness, objectivity, and neutrality of machine reading algorithms both as knowledge appliances and in optimal security decision-making processes. While the gain in speed is undeniable, the gain in accuracy is not so evident, and the assumption of greater objectivity is wildly mistaken, as numerous research studies and cases on the presence of biases in algorithmic decision-making processes have shown.

As Debbie Lisle argues, science and engineering cultures mobilize a politics within which "failure" itself becomes an "instructive experience" (LISLE, 2017). Within a machine learning logic, the enlightening experience of failure and errors allows the model to learn those strange things beyond the data distribution in a training data set. Failure and error are part of the algorithmic learning process, and the acceptance of error as the constitutive part of the learning process undertaken by the machine can tell us about changes not only of methodological, but also of epistemological nature. As we have also seen, there are changes of ontological nature at play in the use made from these technologies to frame security problems. Notably, this research does not aim to debunk or denounce the way algorithms do and act, but to understand how algorithmic truth claims and practices circulate and gain credibility, even amidst controversies about their errors.

Opacity

First, let us start with the criticism that addressed opacity as a problem of machine learning algorithms. These technologies are understood as inscrutable "black boxes" that can only be analyzed in terms of their inputs and outputs (PASQUALE, 2015; INTRONA, 2016). Opacity is problematized both in terms of academic inquiry and for accountability and regulatory purposes (O'NEIL, 2016; EUBANKS, 2017; ZUBOFF, 2019). Based on this concept of opacity, Franck

Pasquale (2015) wrote about the development of a "black box society", when examining the asymmetric distribution of data and information in a world where "unaccountable" algorithms increasingly make decisions hidden behind corporate walls and layers of code. This opacity, in turn, is particularly problematic because algorithms are often biased (BAROCAS; SELBS, 2016): since they are based on historical data, which is shaped by long histories of inequality and discrimination, algorithms can function as "weapons of math destruction" (O'NEIL, 2016) that end up "automating inequality" (EUBANKS, 2017). Not being able to analyze how such biased decisions are made severely threatens the notion of due process in democratic societies (EUBANKS, 2017).

Based on Burrell's (2016) analysis, there are three ways in which algorithms can be opaque:

- Algorithms are typically characterized by intentional secrecy: data and code are kept secret by companies or administrations that guard them as valuable intellectual property. Consequently, observers cannot access algorithms because companies do not make them public.
- Even when companies decide to share their algorithms with users and researchers, another dimension of opacity arises in technical language. Algorithms are made of code written in programming languages; most users have no training to interpret these languages, limiting their understanding of the inner workings of the algorithms.
- Machine learning algorithms have an additional layer of opacity because they evolve in ways that are typically unintelligible to humans, regardless of the humans' training in programming languages.

According to Burrell (2016, p.10), “when a computer learns and consequently constructs its own representation of a classification decision, it does so without regard to human understanding.” Thus, even if we could decipher the codes, we would only be able to partially explain how the algorithms made certain decisions instead of others. In this sense, the metaphor of opening the "black box" to gain insights and transparency about the topography of technology may be a limited approach (MATZNER, 2017, p.44-45).

So far, I have discussed the opacity of algorithms as a practical difficulty. However, describing algorithms as "black boxes" is not a neutral choice. On the contrary, the black box can be analyzed as an artifact of scientific and technological legitimacy, even reinforcing the framing of these technologies as neutral. Latour makes a similar argument when he writes that

> scientific and technical work is rendered invisible by its success. When a machine works efficiently, when an issue is solved, one must focus only on its inputs and outputs and not on its internal complexity. Thus, paradoxically, the more successful science and technology are, the opaquer and obscure they become (LATOUR 1999, p. 304).

As the UK Institute of Mathematics noted in its evidence presented to a House of Commons inquiry into algorithmic decision-making: "no human being can tell why the algorithm does what it does, nor can it predict what it will do with data that is not the training data" (in ARADAU; BLANKE, 2022, p.43). The opacity of machine learning algorithms is not only their generative style and specific thinking and action that is unintelligible and opaque even to their designers, but also an opacity of a multitude of condensed material-discursive practices. Algorithmic materializations are not constructed in a vacuum, or a neutral manner as an algorithmic imaginary of neutrality and objectivity would have us believe (BUCHER, 2017; PASQUALE, 2015). The algorithmic reason holds these multiplicities together as if they were a single possible way out.

Bias, fairness and algorithm errors

Another critique that permeates the academic and public discussion about machine learning algorithms is the problematization of neutrality/objectivity. The supposed algorithmic objectivity is presented as a weapon against controversies, as well as being able to mask its possible misconceptions (GILLESPIE, 2018: 98). As I have pointed throughout this chapter, algorithms are not neutral, despite being framed as such. They are socially produced from certain places and foreground only a particular set of perspectives, at the expense of others. Some important research (NOBLE. 2015; EUBANKS, 2015; O'NEIL, 2016; BENJAMIN, 2019; BROWNE, 2020) has shown how automated decision algorithms are not immune to the biases and asymmetries that are historically present in our societies, in our practices, and in our judgment about the world and others. However, there is an aggravating

factor: racism, chauvinism, class, gender, and race inequalities are, in general, encapsulated, silenced, and invisibilized in algorithmic systems under the mistaken perspective that the machines are making inferences from data reality without the intervention of human hypotheses. Researcher Nicol Turner-Lee, a Center for Technology Innovation member, explains that we can think about algorithmic bias in two main ways: accuracy and impact[28]. For example, a machine learning algorithm, such as facial recognition, may have different accuracy rates for different demographic groups. Similarly, an algorithm can make very different decisions when applied to different populations.

From technical consultancies, Institute of Electrical and Electronics Engineers (IEEE) papers, and big tech companies' reports to government AI plans, they all recognize the so-called algorithmic bias, albeit from different approaches. It is a significant theme in both the academic literature (DIAKOPOULOS, 2014; BAROCAS, SELBST, 2016; ROUVROY, STIEGLER, 2016); and the Non-Governmental Organizations involved in the technology and civil rights debate, such as the Electronic Frontier Foundation, Electronic Privacy Information or The Algorithmic Justice League, American Civil Liberties Union, among others. To be more concrete, it has become common in the algorithmic literature to argue that algorithms can sustain and accelerate oppression (NOBLE, 2018) and reinscribe stereotypes.

A well-known case was the introduction of algorithmic models into sentencing and probation in recent decades in the United States, as the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS). The expectancy was that the growth of crime pattern databases and algorithmic evaluation of recidivism rates would lead to evidence-based, fair sentencing. In this way, the introduction of algorithmic sentencing was supposed to avoid the risk of biases associated with individual judgments in traditional court cases. However, in 2016, ProPublica, a journalism NGO, evaluated the risk scores generated by one such algorithmic system widely used in the US criminal justice system (AGWIN et al., 2016). The assessment showed that the risk scores tended to violate formal non-

[28] Available on: https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency . Accessed on September, 2022.

discrimination legislation, as the system perpetuated social and racial stratification of crime incidence and convictions (AGWIN et al., 2016).

In *Automating Inequality* (2018), Virginia Eubanks shows how the automation of decisions in the United States public service has produced far more punishment and policing of the poor than the practical assistance it purports to provide. Based on three detailed case studies of public services in social assistance, housing, and child protection, she shows how big data and algorithms for decision-making have increased social inequality. We also know that, due to opacity, algorithmic processes are challenging to be negotiated and contest, making it extremely painful to reverse the slightest error or flaw in the system or to solve the smallest problem. Nevertheless, as we have seen, errors and failures are not disruptions, but are part of the optimization process of machine learning algorithms: for the "problems" brought about by the algorithm's, enhanced learning has been advanced as a solution. Here, we see the circular logic of problematization-solution-problem-optimized solution being designed.

Amidst discussions about bias, fairness, and algorithm errors, the response to criticism has been to present possible rules, standards, and formalization within the governance process through an idea of accountability and certification of systems. For example, computer scientists have argued for providing "model cards," short documents for training machine learning models that would include basic metrics on bias, fairness, and inclusion (MITCHELL et al. 2019). Others have suggested adding constraints to algorithmic models to reduce their discriminatory potential. Many of these initiatives have emerged within the intellectual community known as the Association of Computing Machinery Fairness, Accountability, and Transparency.

However, such approaches have, in turn, been criticized for emphasizing "technical fixes" for diagnoses that call our attention to the broad social and political scope of the problem (ABEBE et al. 2020). The focus on "transparency" as an umbrella (ANANNY; CRAWFORD, 2016) and an epistemological approach may consolidate algorithmic opacity rather than diminish it, as the as section 2.1 shows. Understanding how algorithms work mobilizes our attention to the details of producing input and output workflows, that is, what happens in the interim. As Seaver (2017, p.5) observed, by treating the 'inside' of the algorithm as unknowable,

these approaches (e.g., algorithmic audits) participate in enacting an understanding of the algorithm as a black box, knowable only through the relationship between inputs and outputs.

Other approaches have also emphasized decreasing errors and biases by improving databases by making them more diverse. The demand for more diversity in databases and the very shift that extensive technology and platform companies have adopted to "embrace" diversity can be understood as an attempt to respond to the centrality the criticism of algorithmic biases has acquired in public debates. However, according to Hu (2018; 2021), although demographic diversity in databases brings partial solutions, there is no guarantee that algorithms will perform "fairly" in the future. The critical point is that, if there is a need for more diversity, there is a need for increased data extraction. Not all efforts to create a better dataset are ethical, such as Google's purchase of data extraction from radicalized people to make the facial recognition system of its Pixel 4 smartphone more accurate across different demographic groups[29].

According to Hu (2018), the question of building a "just" system is essentially meaningless because these systems attempt to answer social questions that do not necessarily have an objective answer. For example, when used in the criminal system to grant or withhold parole, it does not address the ethical question of whether someone deserves parole. When we insert machine learning algorithms, it does not change the fundamental context of the problem – i.e., that the problem does not have an objective answer. In this sense, it is fundamentally a question of our values and the purpose of the criminal justice system. Thus, no matter how accurate a technology may be, it is not neutral, and there is no guarantee that it is fair.

As we have observed, machine learning algorithms are both productive and contested, encountering friction, breaks, refusal even resistance. As Aradau and Blanke (2022) point out, discussing the implications of these tensions for the "politics of algorithmic reason" is essential to understanding the circulation of these

[29] REED, Rani Molla. How Google's Pixel 4 facial recognition tech was developed with help from black people who were homeless and college students. Recode, 17 Oct. 2019. Available: https://www.vox.com/recode/2019/10/17/20917285/google-pixel-4-facial-recognition-tech-black-people-reset-podcast . Access: 20 May 2024.

technologies and their practical experimentation. These systems are ongoing objects of experimentation: many people are working on the design, implementation, 'tweaking,' and use of the technology. According to Amoore (2022), it is in these moments of experimentation that technology and the way it changes a state of affairs becomes less given as confident and opaque; the technical, practical features and even ethical dilemmas.

In light of the profusion of critiques that has been invested against the assumptions and effects related to the increasing use of machine learning algorithms, this research is concerned with the following question: how can we explain the sustained production and circulation of these technologies in security practices even when they are publicly diagnosed as erroneous and flawed? To explore this problematic, in the next chapters, I analyze specific algorithm that provide empirical support for the thesis on how algorithms have become trusted stabilizers in security practices, and how they have sustained practices that have destabilized what we have understood as efficient and "what works and what does not work" (ARADAU; BLANKE, 2022, p.10; HACKING, 2006). The proposal is to understand algorithmic operations – even when these do not work "perfectly" –, combined with their performative effects, especially in the penal apparatus. Remember, the epistemic coding of algorithmic reason does not revolve around truth and falsity but rather around the efficiency of the algorithmic set. The condition of possibility of the machine learning algorithms' operation and emergence are the multitude and dispersed humans and non-humans' material-discursive practices.

3.
From ‘bio’ to ‘metrics’: how do machine learning algorithms and biometric data produce reliable evidence?

As we noted in the previous chapter, the last decade has seen a significant increase in the use of machine learning algorithms in security practices. The new “data-driven sciences” have provided an enhanced knowledge base for managing individuals and populations (MAYER-SCHONBERG; CUKIER, 2013, p.18), making it possible to “see society in all its complexity through millions of networks of personal exchanges” (PENTLAND, 2015, p.12). Unlike the analog forms of statistical knowledge developed historically in Western societies, actionable knowledge extracted from a mass of data promises to reveal unexpected insights, refine predictive analysis, and identify previously unknown patterns. Moreover, in this sense, algorithms provide a generalizable vision and a technocratic method that reduces deep social issues to optimization problems, i.e., the production of optimizable and efficient responses.

Together with these technologies, the spraying of sensors (cameras and scanners) and the massive collection of ubiquitous biometric data are no longer the realm of futuristic fantasy or dystopia but have been rapidly adopted in various domains and applications for surveillance and security. From the almost 'invisible' implementation of urban furniture in cities to the compulsory passage through airport scanners. The combination of a rapid increase in computing power, available biometric data, and the optimization of algorithms brought about a wave of artificial intelligence research and technologies, especially machine learning algorithms, as well as making biometric data readable and processable in an automated way at scale.

Biometrics is the scientific discipline concerned with measurements and metrics related to biological characteristics (such as fingerprint, DNA facial, iris, or retinal recognition) or human behavioral characteristics commonly possessed by all human beings while highly representative of individual attributes. The biometrics is central to an emerging set of modern policies for determining someone's identity. Establishing and authenticating identity is key to achieving various goals, from

catching criminals to establishing efficiencies in the health and social security sector to providing an identity deemed trustworthy enough to open a bank account. The possibility of authenticating individuals based on their physical or behavioral characteristics brings a layer of "security," making it easier to cross-reference sources for identity recognition and verification. When establishing the trustworthiness of strangers, an iris scan, facial images, or a database of DNA samples and fingerprints is faster and more "reliable" than a story told in an interview, for example.

So, if one follows the discursive rationale that biometric characteristics do not lie, one takes that they tell the truth about someone's identity. Simone Browne (2010, p.135) offers us the idea of "digital epidermialization" to think about how biometric surveillance rewrites the "body as evidence" by searching for the supposed answer embedded in the body by "illuminating" the subject to produce a truth about them through scientific rationality codified through the analysis of algorithms (BROWNE, 2010, p.135).

With the possibility of biometric data being analyzed by machine learning algorithms, the body can speak the "truth" through the "unequivocal and enigmatic language of algorithmic codes" (AAS, 2006, p.154). As Aas (2006) argues, the question is what kind of ‘truth’ the biometric data analyzed by algorithms is telling us. Biometrics fixes the physical body as the “profession of truth” (BROWNE, 2010), and algorithmic analysis of this data determines the limits of identification and recognition of authentic identity. Suppose our bodies function as passwords in the analysis processes of these biometric technologies. In that case, they enter a binary universe of acceptance or denial of identity based on algorithmic understandings of digitized body data. It is possible because there is trust in the algorithmic responses and the exclusion of doubt with the use of biometric data.

Establishing this trust in both algorithmic processes and biometric data is a fundamental aspect of the discussions that advocate the superior efficacy of biometric solutions for identification and security concerns. To address the queries, I have grappled with in this dissertation, it is imperative to scrutinize how security and legal professionals develop trust in specific evidence based on algorithmic

analysis of biometric data. What do algorithms enable us to consider in terms of solutions that are sufficiently efficient?

The readability, translation, and processing of biometric data by machine learning algorithms are essential for the proposed analysis. Biometric data analyzed in an automated way brings together both the idea of producing a true identity through “bio”, bodily evidence, and an objective way of measuring this identity through algorithmic calculation, which is understood to be more efficient. This chapter aims to map the history and entanglement between the production of biometric data and machine learning algorithms as 'sufficiently efficient' solutions for dealing with security issues, producing order, amid uncertainty.

In this sense, I propose to explore the effects of the growing use of biometric algorithms, such as facial recognition, by security agencies not despite the discourse of efficiency and objectivity but as implications that are authorized and made legitimate precisely because of the political force of this discourse. The idea is to offer reflections that question what biometric algorithms do and how they do it and consider how they work as part of a broader entanglement of processes involving humans, algorithms, data, and infrastructures. Furthermore, how these entanglements circulate, (re)produce, and stabilize themselves as a reliable apparatus for attribution, recognition, and identification.

To do this, I will first briefly analyze the mapping of the connections between the use of biometric data to recognize social "anomalies" and the development of entangled scientific and security practices. This point is fundamental to understanding the foundations of the development of biometric technology automated by algorithms that I will be analyzing: facial recognition. It also places facial recognition algorithms in a long-standing context of calculative technologies made available to the state to deal with disorder.

Following, I will pay attention to the trust placed in the algorithmic processing of biometric data. The assemblage and stabilization of this trust are of interest in our analysis precisely because they reveal the regime of truth constituted by and through these technologies. If we consider that the term algorithm carries something of an authority because it is "trustworthy," we need to think of it as part

of a knowledge apparatus through which power relations themselves are performed, reproduced, and normalized.

After that, I will look at the example of biometric facial recognition algorithms and their uses and effects. It is worth pointing out that this is not a deep dive – that will be done in more detail in chapters 4 and 5 – but a necessary framework for understanding how automated facial recognition technologies (FRT) work. In analyzing FRT, it is essential to understand a set of contributions that have sought to reveal the inseparable nature between these technologies and social processes (SEAVER, 2013, p.10).

In this sense, it is essential to analyze how biometric systems and the penal system are entangled and what place biometric algorithmic technologies have occupied in framing what is understood and recognized as an "anomaly" that needs to be governed to maintain order. Therefore, I propose to draw attention to how the mode of 'telling' and 'showing' the truth told by algorithms based on biometric data is intertwined with security and knowledge production practices and what they make possible.

3.1. Biometric data: legibility and recognition of “abnormality”

Biometrics does not emerge from a singular origin but from a complex history that intertwines political, social, and technical-scientific development factors (PUGLIESE, 2012, p.25). Biometric data linked to the analysis of machine learning algorithms has the idea of fixing the body, or instead, its mathematical and digital coding, as the actual evidence of who is or claims to be (PUGLIESE, 2012; BROWNE, 2015). There is a translation of life into patterns of information, disembodied and elevated to new levels of abstraction (HAYLES, 1999). In this sense, algorithms with biometric data have framed how we are treated and presented as objects of attention, recognized, and read.

Over the years, biometrics has been seen as a technical-scientific solution to the growing need to identify and recognize individuals and social groups (LYON, 2008, p.500). This identification underpins the development trajectories and operational adoption of some of the most significant and controversial social control technologies. Included here are the rapid growth of biometrics, such as the UK's

National DNA Database, and the proliferation of surveillance and facial recognition technologies (FUSSEY; DAVIS; INNES, 2021). Biometric identification technologies have been "vital in identifying undesirable populations in the new global order" (AAS, 2006, 145-146).

The use of biometric data has become an integral part of identity management systems worldwide, where many people do not have formal identity documents to prove who they are. The World Bank maintains a list of all jurisdictions and levels of development of biometric identity documents and systems[30]. The Aadhar project, implemented by the Unique Identification Authority of India (UIDAI), is an example of an unprecedented effort to provide a unique 12-digit identification number to approximately 1.2 billion residents of India (TANWAR et al., 2019). This project uses fingerprints and iris prints to eliminate duplicate identities. Such biometric identification programs are expected to serve as vehicles for effective healthcare delivery, reduce welfare benefits fraud, and enable secure financial transactions (NAIR, 2021).

Biometric systems have also changed how we travel, aiming to increase border crossing systems' security, efficiency, and reliability. In the US, for example, biometric-based authentication of people in border control and transportation systems was implemented after the September 11 terrorist attacks. This technology is increasing in our daily lives through consumer electronics; all the major mobile device providers have now incorporated or are introducing biometric-based authentication for smartphone security and payment. It also uses biometric recognition in applications such as Facebook and Google Photos.

Biometric systems identify, recognize, authenticate, and authorize quickly, are perceived as efficient, and are tools for classifying individuals (PUGLIESE, 2010). The ability to prove that you are who you say you are allows access to many public and private sector services and allows the expansion of surveillance devices on individuals and groups. The identification imperative so latent with the growing use of biometric technologies reveals an ambivalence: the combination of both a power over the individual, with practices of surveillance and coercion, and a power for the individual to be recognized (FOCAULT, 1988). It is because security and

[30] WORLD BANK. ID4D Dataset. Available on: http://data.worldbank.org/data-catalog/id4d-dataset . Accessed on: 11 Nov. 2021.

governance depend on identifying the population, which increasingly relies on biometrics as a reliable form of identity authentication (LYON, 2008), an authenticity anchored in the "truth" of a single, verifiable identity. Following this line of argument, biometric characteristics are understood as a source of precision (AAS, 2006; LYNCH, 2008) in which "codable" bodies authenticate passwords. In this process, the body is as much an object of surveillance as it is of identification and recognition (LYON, 2001).

Suppose our bodies function as passwords in the analysis processes of these biometric technologies. In that case, they enter a binary universe of acceptance or denial of identity based on algorithmic understandings of digitized body data. It is possible because there is trust in the algorithmic responses and the 'truth' in the biometric data. Building this trust in algorithmic processes and biometric data is an essential part of the discourses claiming the superior effectiveness of biometric solutions in dealing with persistent security problems. So, it is essential to return to the questions that permeate this diseertation: how do security and legal professionals trust specific evidence based on algorithmic analysis of biometric data?

Biometric identification automated by algorithms presents some novelties in the history of biometric practices and simultaneously confirms some continuities (LYON, 2008). For this reason, in this section, I will briefly analyze the historical processes involved in producing biometric techniques and the entanglements with the analytical techniques on which machine learning algorithms are based. One important point is that correlation, linear regression, pattern recognition, and other foundational statistical methods for the operation of machine learning algorithms have their development roots associated with research by eugenicist biometricians and statistical mathematics in the 20th century (CHUN, 2021, p. 44-45). As Kate Crawford (2021) reminds us, if algorithms are present in a logic of knowledge and how we are framing and understanding contemporary problems, then it is essential to consider the contours of this logic and what histories and philosophies it has been shaped by. So, here, I take a long history of social knowledge production seriously through measurement systems, both at the level of groups and individuals, and I believe that new classifications and enumerations are inseparable (HACKING, 1990).

Legibility and recognition of "abnormality"

The first known research publication on automated biometric recognition was published by Trauring in 1963 on fingerprint matching. The foundation for automated biometric systems based on other characteristics such as voice, face, and signature were laid in the 1960s (JAIN; ROSS, 2015). Not surprisingly, the advent of biometric recognition systems coincided with advances in other closely related areas, such as artificial intelligence, pattern recognition, and image processing in the 1960s, which collaborated in the analysis and recognition of biometric patterns in an automated way (JAIN; ROSS, 2015; CRAWFORD, 2021), as we described and analyzed in chapter 2.

However, the event that truly marked the systematic use of biometric characteristics to recognize a person happened a hundred years before Trauring's landmark article. This pivotal event was the enactment of the Habitual Criminals Act in 1869 in the United Kingdom. This law, a significant step in the history of biometric recognition, made it compulsory to keep a register of all people convicted of a crime, together with appropriate evidence of their identity (DAUGMAN, 2003). This register was used to identify repeat offenders, who were generally imprisoned with a higher degree of punishment compared to first-time defendants.

Also, French detective Alphonse Bertillon introduced a system for recognizing people based on a set of anthropometric measurements to identify repeat offenders. Since the 1870s, French criminal archives have incorporated photographic portraits, a technology that made it possible to sophisticate the set of identification data until then limited to written records of age, height, skin color, scars, tattoos, and other particular marks. Photography was a great ally in the identification process, but it did not offer any advantages when it came to classifying files, which continued to depend on alphabetical order. Aware of this problem, Bertillon began experimenting with a new classification method based on the body measurements of detainees.

This method was seen as a means of classifying and discriminating between the records of individuals and researching between them (JAIN; ROSS, 2015), and established a set of standards for forensic photography. He also developed a

taxonomy to describe some of the physiological features of the head, including nose, forehead, and ear. It became known as the parle portrait (talking portrait) (BERTILLON, 1980). The combination of anthropometric measurements and the talking portrait developed by Bertillon is the so-called Bertillonage methodology and was quickly adopted by the French police and judicial system. The carnet anthropométrique, for example, issued in France in 1912, was a "solution" to help the police deal with the problem of repeat offending, but it was also used against gypsies and nomadic bohemians as a "technique of republican government aimed at society in general" (BOWKER; STAR, 1999). It is worth noting that the idea that deviance and risk can be read in some way from the body was not new, but it was acquiring methodological sophistication.

In Berillon's method, repeated measurements converged on the average, which became the measure of true knowledge, and the combination of body measurements would make individuals uniquely identifiable (ARADAU; BLANKE, 2021). In search of precision, Bertillon identified two forms of error: an error of measurement and an error of interpretation. The difference between the measurements should not exceed "the approximation" indicated for each measurement, and the second source of error arose concerning the subjectivity of the operator, both in the skill and use of the measuring instruments and in reading the “suspect” (ARADAU; BLANKE, 2021). As Cole (2012, p. 36) explained, “[t]he recording of anthropometric measurements was an elaborate dance. Controlling error required human skill to use instruments in a standardized way.”

As we can see, the Bertillon system lacked automation, was challenging to administer uniformly (which made it prone to errors), and even when administered correctly, the measurements were not distinct enough to uniquely identify individuals (JAIN; ROSS, 2015). For this reason, the method was sidelined in favor of a relatively simpler, more efficient, and "accurate" approach involving the manual comparison of human fingerprints. Fingerprint biometrics as a form of identification was made possible thanks to the pioneering work of Faulds, Herschel, and Galton. They studied how to distinguish the configurations of specific characteristics in a fingerprint pattern, such as tiny dots. Fingerprints soon replaced anthropometry due to their ease of obtaining, identifying, and retrieving (DIXON, 2015; CHAMPOD; TISTARELLI, 2017). It is important to stress that although

there were several reasons for replacing Bertillon's anthropometry with Galton's fingerprint, the error was problematized in the competition between their methodological approaches (ARADAU; BLANKE, 2021). In other words, adoption at scale was preferable to the most efficient methodology in terms of identification. However, it should be noted that efficient does not mean 'perfect', but useful.

Fingerprinting, also had one of its pioneering uses in distinguishing between members of groups considered racially homogeneous, such as blacks, indigenous people, and the Chinese community in the United States, for example (PARENTI, 2003). In his study on “suspicious identities,” Cole (2001, p.139) concludes that while anthropometry prided itself on being carefully scientific, fingerprinting was seen as a technology applied to the masses to be policed and surveilled. According to Cole (2001), this practice was imported from its use in the British colonial administration in India, where Herschel pioneered its use in Bengal. Herschel traced the genesis of the modern fingerprint and its encounter with “native” signatures. He wrote about his experiences for Francis Galton, a statistician and founding figure of eugenics, who at that time was already conducting research in institutions such as the army, hospitals, asylums, and prisons to trace hereditary characteristics of “race” and their relationship with human behavior (COLE, 2001; MAGUIRE, 2009; CHUN, 2021).

Francis Galton outlined a standardizing and disciplining apparatus for error in fingerprint collection and analysis (ARADAU; BLANKE, 2021). The Galtonian method apparently avoided errors due to the operator's subjectivity and the skill required by Bertillon's anthropometry (JAIN; ROSS, 2015). According to Aradau and Blanke (2021, p.11), the discourse of precision of the fingerprint method circulated in the public imagination, “this was the fragile effect of a device carefully calibrated to control error.” The error seems residual in historical analyses of biometric technologies, probably, as Aradau and Blanke (2021) argue, as probabilistic reasoning shifted the emphasis from the “law of error” to an idea of normal distribution. According to Makenzie (1976 apud ARADAU; BLANKE, 2021), the variability of error for Galton could potentially be desirable in his statistical analyses; error did not need to be eliminated but tamed. Although anthropometry was implemented in the metropolis, it was only much later that

fingerprinting became a general technique for identifying the population as a whole, as it met with resistance, not because of its accuracy, but because of its association with abjection, criminality, and the colonial imaginary (BRECKENRIDGE, 2014).

Furthermore, in the 1870s, Galton carried out experiments using a method of photographic analysis of the British prison population. He tried to create a composite image of the "average man" by superimposing facial images of group members. As the prison population grew, so did a systematic photographic archive, which promised to capture the habitual criminal (MAGUIRE, 2003) literally. As noted earlier, Bertillon saw the photograph as a kind of biographical identification machine needed to detect repeat offenders. However, Galton's experiments with prisoner photographs aimed to detect a biologically determined picture of "prisoner types" (CRAWFORD, 2021, p.91-92).

Galton was working on a physiognomist paradigm in which the central idea was to discover a 'scientific look' through statistics that could be used to identify character traits through appearance. It is essential to point out that phrenology (the study of the conformation of the skull as an indication of mental faculties and character traits) and physiognomy had already been criticized and presented scientific controversies at the time of Galton's experiments with photographs (CRAWFORD, 2021). The "objectivity" of Galton's photography was anchored in his statistical tool for investigating his hypotheses of biological degeneration (GOLDENDEIN, 2019, p. 115).

Galton's concept of correlation emerged from his dispute with Bertillon over the best way to identify criminals using anthropometric methods (ARADAU; BLANKE, 2022). Galton believed that some of Bertillon's measurements, such as the length of a person's arm and leg, were linked and, therefore, redundant. He produced a coefficient linking these variables to prove that these measurements were not independent.

In this version, correlation (a version more commonly used in statistics) is used to reduce the number of variables involved rather than to uncover "hidden" or latent variables (CHUN, 2021, p.74). According to Hacking (2006, p. 149), Galton "provided the first statistical explanation of a phenomenon" (as opposed to a singular fact). The 'novelty' of Galton's explanation of population phenomena

through correlation was made possible by consolidating the statistical analysis method of population regularities and calculating probabilities advanced by Quetelet's discovery in 1844 (HACKING, 2006). From creating a new 'object' (concept), namely the notion of the population using a mean and standard deviation, parameterization becomes possible, guaranteeing objectivity to the measurement method, parameterization, and quantification (HACKING, 2006, p. 148).

Galton and Karl Pearson developed the concept of correlation and linear regression in statistics in their attempts to determine heredity in "Typical Laws of Heredity in Man" (1877). Statistical regressions captured the past through discrete sets of anthropometric information while asserting methods of analysis and interpretation, which subjugated "types of people" and reaffirmed a kind of mastery and knowing about the future – which could be given its hereditary component (CHUN, 2021). In this mode of analysis, both the past and the future were linked to statistical processes abstracted in mathematical logic. Anthropometry gained a foothold in the expanding eugenics movement, which made possible a social policy around biological and physical human differences stabilized by new mathematical calculation methods (DRYER, 2019).

According to Dryer (2019), the widespread adoption of linear regression and correlation architectures set an important precedent for the emergence of mathematical statistics in the 20th century, establishing mathematical authority to the mechanisms for governing social, political, and economic systems that made today's techno-scientific development possible as such. Arguably, linear regression analysis itself can be considered algorithmic, as it is a mechanical mode of data collection and processing that dictates a precise order for its calculation and interpretation, whether computational or not (MARLAD; ABDULAZEEZ, 2020; NASEM; TOGNERI; BENNAMOUN, 2010).

In this emerging context, detecting patterns based on calculations was already becoming a way of thinking about the world (KAUFMANN, 2019). As I noted in the previous chapter, pattern identification emerges from successive negotiations about what counts as reality and what knowledge apparatuses are used to analyze it. Identifying patterns, together with the apparatuses and the meanings and interpretations drawn from them, affect our perceptions of phenomena and the possibilities of what they can be and how to resolve them.

The "bio" and the "metrics"

As an apparatus of knowledge, statistics required stabilizing scientific trust in its technical meanings and practical applications, which materialized through different material-discursive intra-actions. According to Dryer (2019), this logic of trust reinforced the authority of numbers in the social and political world. In Galton's universe, trust was a statistical and affective concept referring to his confidence in the specific linear regression analysis technique, which ensured that he could draw general laws or hereditary conclusions from his data. The eugenics movement was a philosophy and social ideology deeply stabilized by seemingly banal administrative procedures and stabilizing calculations of scientific confidence (CHUN, 2021; CRAWFORD, 2021; DRYER, 2019).

Trust is produced, reproduced, and stabilized through mundane and dispersed practices. According to Hacking (1992, p.181), styles of reasoning – ways of thinking and doing scientific apparatuses, in the language of Barad (2007) – which are eminently public, are part of what we need to understand what we mean by objectivity. These 'styles' have established what it is to be objective: what kinds of truths we obtain by conducting certain kinds of investigations and meeting certain standards. In other words, these 'styles' define what it is to be objective because, when a way of thinking and doing emerges, it introduces a set of novelties, particularly a new type of evidence. This new form of evidence provides the new criteria by which new sentences become candidates for truth or falsity (HACKING, 2002, p. 160). Thus, a truth or falsehood is analyzed according to a specific standard of style of what is ultimately considered science.

This is why the production of scientific apparatuses and their circulation, adherence, and remodeling are central to this dissertation. Science, and the very idea of what we understand about science, circulates by simplifying complexity. It produces inscriptions that make complex phenomena flat, readable, portable, and treatable (LATOUR; WOOLGAR, 1979); it can produce "useful truths" to inform policies and practices (JASANOFF, 2015).

The publication and creation of journals are examples of the importance of circulation for the production of apparatuses for establishing practices and styles of reasoning. This was an important step in popularizing the methods that fused

statistics with the biological analyses proposed by the eugenicists. In 1901, Karl Pearson and zoologist Raphael Weldon founded the mathematical statistics journal Biometrika, which aimed to publish and distribute statistical methods for analyzing biological and social phenomena throughout the 20th century.

The main focus of Biometrika was the circulation of biometric data and a statistical data system to elucidate the idea of human difference. Through statistical analysis, eugenic ideas gained legitimacy as a program was mathematically proven (CRAWFORD, 2021). The publication of academic debates was essential for the circulation of eugenic methods and ideas, as well as the creation of a network of researchers beyond England, such as the pioneer of eugenic thought in the United States, Charles Benedict Davenport (GILLHAM, 2001, p.97). The primacy of eugenics for the journal's program is stated in the first paragraph of Biometrika:

> The first step in an investigation into the possible effect of a selective process on any character of a race should be an estimate of the frequency with which individuals, exhibiting any given degree of abnormality in relation to that character, occur. (Editorial, "The Scope of Biometrika". Biometrika 1, no. 1 (1901) apud DRYER, 2019, p.45-46).

At the turn of the century, statistics became a field that turned statistics into a "coherent science" through the affirmation of laws of counting, measuring, and estimating on data designations: biological data, heredity data, and anthropometric data (DRYER; 2019; HACKING 2006). Analyses based on Pearson's statistical calculations, such as the chi-square test, standard deviation, correlation, and regression techniques, are considered fundamental data organization methods.

These methods of analysis circulated in publications and were widely and rapidly adopted by networks of experts in social planning, biometrics, medical analysis, bacteriology, food studies, and so on (DRYER, 2019). They were integrated into information work in the same way as they were being elaborated in academic environments. Biological data and regression methods were the fundamental components of the "new mathematics," which spread into new applications and contexts through the interwar mathematical statistics movement (DRYER, 2019; CRAWFORD, 2021), as we also noted in section 2.2 its importance in the development of the field of artificial intelligence.

As a method, correlation promised to be helpful in all scientific fields, especially those where it was problematic to establish casualty guidelines. It is because the concept of correlation broadened the possibility of knowledge beyond causality; in other words, it establishes another way of building explanatory knowledge about phenomena that does not imply a cause-and-effect relationship between variables. Correlative reasoning linked to biological data analysis, especially biometric analysis, claimed to make living beings and human behavior mathematically understandable. In this way, human behavior would be explained by hereditary biological information and not by characteristics of their mode of socialization or social environment.

The correlation was the key to "proving" that behavioral variables were natural/hereditary and not social (CHUN, 2021, p.61). This created the conditions for categorizing "types of people" and their generalization. Through the delineation of categories and their biological characteristics, the possibility of repeating a behavior expected of others with similar attributes is parameterized, given that what explains behavior (for this group of academics) are biological variables.

As Chun (2021) argues, correlation was never simply about discovering similarities between variables but also about biological similarities to propose an "order" for the future. This order is established and perpetuated by limiting the possibilities of being something to an expected way of being understood through repetitions of past actions. We see here that the eugenicist history of correlation is important, not because it predisposes all uses of correlation for eugenics, but because when correlation works, it does so by making the present and the future coincide with past data. Eugenicists have reconstructed a past to project a future that would repeat their discriminatory abstractions in their systems. The learnings or differences would be deviations and noise that must be addressed.

The correlative method, in its historical and political trajectory, is linked to practices of association and standardization (HACKING, 2006), as observed in eugenicist analyses. According to Hacking (1990), the concepts of correlation, variability, and uncertainty, which play a central role in our ways of thinking about our contemporary experience, are expressed and conceived in probability. As we analyzed in section 2.2, with the space of possibilities opened up by the concept of probability, scientific discourse emerged with its conceptual material, its practices,

and its theoretical structures. In this discourse, uncertainty is thought of as standard deviation, defined as a probability distribution.

Probability suggests that the newly formed statistical worlds (political, economic, physical, biological) can and should be understood in probabilistic structures. According to Dryer (2019), whether probability as a language and mode of knowledge should reign over these worlds was the dilemma between academia and policymakers, and there was no consensus. Accepting the probabilistic worldview means that knowledge can never be absolute, as "knowledge" is reduced to a translation of likelihoods. However, rejecting the probabilistic view also meant that knowledge could never be absolute, as it was believed there would never be a unified mathematical description to measure the world. This indeterminacy about uncertainty constituted the problematization of probability, a double-layered doubt that contributed to the anxiety of post-World War II society (DRYER, 2019, p. 45-46).

As Jasanoff (2004) argues, the co-production of social order and technoscience characterizes technical development, laws, and political relations that facilitate and implicate each other. By the end of the 1930s, the techniques of linear regression, standard deviation, and correlation would become dominant tools used in understanding and interpreting social and state information on the world stage, as would the use of biometric data (DRYER, 2019, p.266-268). Statistics became a vast undertaking, not only academic but also practical, which expanded after the Second World War with the use of computer systems, as we analyzed earlier.

Uncertainty and anxiety, as Amoore (2019) argues, came to be thought of in terms of a probability distribution. The probabilistic way of thinking and doing becomes part of what we need to understand and what we understand as objective (HACKING, 1992, p.181). In his argument, Ian Hacking (1992) offers an idea of "inevitability" because we now cannot conceive of the world without the concept of probability: it organizes how we organize our thinking and how strongly we believe that something will happen. The resource introduced by probability is epistemic and ontological and refers to our knowledge and beliefs about facts in the world and the facts themselves (ROBERTS; STOCKDALE, 2018).

Visions of desirable futures are collectively held, institutionally stabilized, and publicly executed, animated by shared understandings of forms of social life and social order achievable through and conducive to advances in science and technology (JASANOFF, 2015, p.4). The relationship between science and the production of forms of (in)security and (dis)order emerges through and as part of an intra-action in socio-material arrangements made possible. As described, the 'abnormal' must be identified to produce order and guarantee a secure future. Moreover, the perception and identification of the standard deviation became possible due to a correlative way of thinking and doing that emerged entangled with the idea that the 'bio' would contain the degree of truth necessary for calculating probabilities. In other words, biometrics is a reliable way of identifying and attributing perceptions about an individual or population.

Mathematical objectivity and technical reproducibility principles have invested biometrics with the idea of authority and credibility in identifying and authenticating individuals. This assumption that biometrics is linked directly to physical bodies conceals complex technological processes of mediation and translation and a whole set of material-discursive practices that create the very conditions of possibility for biometric practice. In this brief historical analysis, I have argued that figures such as Herchel, Galton Bertillon, and Person did not simply "create" technologies and modes of human identification, classification, and data archiving. However, each outlined possibilities for the emergence of biometric security systems in their own time (MAGUIRE, 2019).

Contemporary biometric technologies, such as computer-based facial recognition and biometric techniques, merged Bertillon and Galton's projects. Both in the way of "authenticating" the individual and the type, they seek to produce "authenticity machines" (CHUN, 2021). According to Chun (2021), Galton's and Bertillon's systems, however, were never truly separate since the goal of recognizing criminals assumed in advance a stable category of individuals classified as "criminals" whose characters did not change, even if their appearances did. As discussed, Galton formulated the correlation in response to Bertillon's method, which he believed to be complicated to apply in practice.

As analyzed, the history of the development of biometric technologies shows more than simply periods of technical-scientific innovation; it also shows the

relationship between accuracy and errors and varying levels of public acceptance and credibility. Biometric solutions, such as Bertillon and Galton's analog anthropometric methods, once considered efficient and scientific methods of identifying and authenticating individuals and groups, are now framed by some authors as "historical curiosities" (MAGUIRE, 2009).

However, looking at the historical development of biometric technologies and the production of knowledge in which it is entangled helps us to understand how biometrics is not only the future and present of security and surveillance practices, as it is commonly referred to, but it is also their past. As analyzed, the introduction of bertillonage systems and criminal convictions based on biometric data (such as fingerprints and DNA evidence) began to pave the way for a thinking and doing security, which machine learning algorithms are now part of.

Furthermore, the reading offered in this section also indicates that the emergence of biometric recognition is intertwined with the practices of monitoring and policing "suspicious" populations, the asymmetries of power, and the violent colonial legacy. In these practices, 'recognition' involved identifying and apprehending suspects and criminals and the classification of 'types' of people perceived as at risk,' 'savages' – prone to degeneration or not even considered human. The introduction of anthropometric systems and the development of biometric technologies introduce a mode of thinking and doing security centered on identifying abnormality through increased registration (expansion of the database) and modes of identification and classification (improvement of biometric technologies). This practice was aligned with the "sciences that terrorized marginalized bodies" (PARENTI, 2003, 51).

The very condition of possibility for the development of contemporary technologies that make bodies visible and legible, such as fingerprint scanners and facial recognition algorithms, are entangled with power asymmetries and deeply racialized political-social structures (BENJAMIN, 2019; BROWNIE, 2010; CHUN, 2021). Through a discourse of externality and neutrality of algorithmic reason, trust in the processing of biometric data by these technologies has been sedimented. In this disertation, I reinforce those algorithms are not external or neutral but deeply entangled by socio-material conditions and social, philosophical, political, imaginative, and symbolic implications.

3.2. Automation of biometric data: the reliability in the processing of biometric data by machine learning algorithms

As we have seen, there is an idea that biometric data tells the true story of who we are and even what we can be. According to this logic, the body has an absolute truth discovered through its digitized measurements, which are analyzed contemporaneously by algorithms capable of processing many biometric records. For this reason, just as important as increasing the number of biometric data records is the use of algorithms capable of analyzing them in a technical-scientific and objective way, but also in an efficient and practical way to solve security problems. It is why this section aims to discuss how the reliability attributed to algorithmic processes powered by biometric data impacts the production of a way of telling the truth about someone's identity.

Currently, we still see the stabilization and continuity of previous biometric methods that also used pattern recognition in biometric data (such as photographs, body metrics, and fingerprints); however, the difference is that we now have more and more data available and greater computing capacity to process the data through algorithms. As analyzed in section 2.2, cloud computing, data, and advances in machine learning through algorithms have made what is almost "seen" perceptible and actionable, what would otherwise be beyond the threshold of human vision and processing capacity.

The development of automated biometric recognition models can use statistical methodologies that date back to the origins of the field of biometrics. However, as Chun (2021, p. 223) argues, one of the most direct links between automated biometric methods and the first biometric methods we looked at in the previous section is the construction of image banks to determine "typical faces." The ability to discriminate, distinguish, and classify is the historical parameter for recognition (CHUN, 2021, p. 224).

As I pointed in the previous section, Galton used analog techniques of superimposing faces to recognize facial patterns. Imagine the amount of time committed to a single Galtonian analysis and the limited database of photographs since photographic records were not yet so commonly used. With computing and transforming images and fingerprints into data to be read by machines and then

processed by algorithms, biometrics could be automated and no longer depend on analog human measurements (ARADAU; BLANKE, 2021).

The first research into automated facial recognition took place in the 1960s, a time, as we analyzed in chapter 2, of growing investment in the emerging field of artificial intelligence and the use of computer technologies for security. In 1964, scientist Woody Bledsoe began experiments in translating face patterns into data, primarily funded by the Central Intelligence Agency (CIA) for the future use of the technology for security purposes. Bledsoe's pioneering experiments were based on methods of algebraically comparing distances between facial features. The research brought together the anthropometric idea of the mediation of bodily characteristics as an essential variable for identifying an individual with the computational statistical methods that were being developed. According to Raviv (2020), Bledsoe attempted to create a fully automated Bertillon system for face recognition and identification.

Unlike today, where researchers and developers can access a range of public and private databases of already digitized photos, Bledsoe's team needed to build a digital database – one photo at a time. The team used 2,000 images from a police photo book to create their database and automatically compared new photos to detect similarities[31]. To do this, they marked facial features and locations, such as the mouth, nose, or eyes, using a RAND tablet[32], which could record the coordinates on a grid. These coordinates were drawn on the distance lines between the center points of the facial features, and a facial geometry was formed that was digitized.

In his method, Bledsoe combined analog (such as the mathematical notation in his database of non-digital photos that would be digitized) and digital analyses with statistical computer models that made it possible to construct a list of twenty standard distances between the points of the facial geometry. Essentially, the method aimed to teach the computer to process the measurements of the facial distances (in other words, to process the numbers) to determine a specific face. It is important to note that the distances were calculated and stored in the computer along with the individual's ID. Hence, Bledsoe's research intended to provide a

[31] Woodrow Bledsoe Originates Automated Facial Recognition : History of Information. Available at: https://www.historyofinformation.com/detail.php?entryid=2495 . Accessed on: May 20, 2024.
[32] The RAND Tablet is a graphical computer input device developed by The RAND Corporation.

computer with a database of different people's faces and see if the computer could recognize new photos of the individuals in this database.

In summary, the development of automated facial recognition research has its trajectory entangled with understanding body characteristics encoded in numbers as an optimized way of identifying and recognizing individuals through facial features. The first automated facial recognition methodologies, greatly influenced by Bledsoe's research, are based on geometric features that depend on measurements between specific facial reference points. As we noted earlier, this method is inspired by the analog anthropometric method of forensic face recognition.

Takeo Kanade, in his 1973 doctoral thesis, was the first to develop an automatic facial recognition system. The first fully automated facial recognition algorithm was still based on the methodology of facial geometry (features). Kanede used digital image processing methods to extract a vector of 16 parameters: proportions between distances, areas, and angles, and used Euclidean distances to compare, achieving a performance of 75% on a database of 20 different people, using 2 images per person (KANEDE, 1973). Despite the performance rate and the limited database, i.e., the low operational accuracy of the algorithm, Kanade's (1973) research is central to advancing research with statistical models for the development of computer vision algorithms.

According to Zao et al. (2003), there was a significant growth in research into automated facial recognition in the 1990s, which can be attributed to the increase in interest and commercial opportunities for applying the technology, the availability of real-time hardware, and the growing importance of devices related to surveillance and security. There was a movement towards both an increase in the number of studies and a technical-scientific advance towards making facial recognition methods fully automatic and more effective, given that the experiments had high false identification and non-identification rates concerning the database.

In this sense, the more straightforward feature methods gave way to principal component analysis (PCA)[33] approaches, linear subspace, and statistical

[33] Principal Component Analysis (PCA) is a mathematical procedure that uses an orthogonal transformation (orthogonalization of vectors) to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables called principal components (ABDI;

models that became mainstream for developing automated facial recognition algorithm methods and models. PCA, a statistical method also developed by eugenic biometricians, led to one of the most significant advances of the late 20th century in facial recognition technology: the eigenface method, which moved facial recognition technology away from human determination towards algorithmically determined features (CHUN, 2021). It is no coincidence that facial recognition research begins with anthropometry. The links between anthropometry and recent studies into facial recognition technology are topical, and their methodologies are markedly entangled. Since then, statistical and probabilistic tools have been used to solve automated facial recognition problems, and one of the popular methods is eigenface (ZAO et al., 2003).

The *eigenface* method, developed by Sirovich and Kirby (1988), showed that analyzing features in a collection of facial images could form a set of basic features by applying linear regression. In the early 1990s, the so-called "eigenfaces" provided a new way of automatically recognizing faces by reducing the statistical extensions of a facial image (ZAO et al., 2003). The eigenface method was a technique for dealing with the high dimensionality of facial images and reducing errors by focusing on the important pixel values, but not all of them simultaneously. Thus, they represented faces as vectors in a feature space so computers could start to identify relevant features and process images much faster (ZAO et al., 2003)[34]. A variation of the eigenface approach attracted public attention in January 2001 during an experimental deployment at the Super Bowl in the United States to identify faces from surveillance footage and compare them with digital photos (ARADAU; BLANKE, 2021; GOLDENFEIN, 2019; CRAWFORD, 2021).

The advance of automated biometric research has increasingly required the expansion of available digitized biometric databases. A central example that marks a way of "doing data" before the Internet offered a way of mass data extraction was the funding by the US Defense Advanced Research Projects Agency (DARPA) – specifically, the Department of Defense's Counterdrug Technology Development

WILLIAMS, 2010, p. 433-445). In summary, PCA is an analysis method that can be used to analyze interrelationships among a large number of variables. In addition, explain these variables in terms of their inherent dimensions (components), in which the goal is to find a way to condense the information contained in several original variables into a smaller set of statistical variables (components) with minimal loss of information.

[34] A systematic survey of automatic face recognition can be found in the work of Zhao et al. (2003).

program office – and the National Institute of Standards and Technology (NIST) of the Facial Recognition Technology (FERET) program in the early 1990s to stimulate the commercial facial recognition market. The expansion of investments in databases for facial recognition research took place in the context of a few databases of digitized images with good resolution available that were not sufficient for the development and application of facial recognition technology at scale (CRAWFORD, 2021, p. 104).

The FERET project involved creating a database of facial images. The test set included 2,413 static images of the face, representing 856 people. The hope was that a large database of test images for facial recognition would inspire innovation and could result in more powerful facial recognition technology (CRAWFORD, 2021). It is important to note that for more than 50 years, NIST (one of the oldest laboratories in the USA, now part of the Department of Commerce) has collaborated with the Federal Bureau of Investigations (FBI) in collecting, automating, and analyzing biometric data (CRAWFORD, 2021, p. 91). After the terrorist attacks of September 11, 2001, NIST became part of the US national response in creating biometric verification standards, not only for law enforcement and secret services but also for surveillance and monitoring people's movements at borders (CRAWFORD, 2021, p. 96).

In addition, following the terrorist attacks, the International Biometrics Industry Association[35] released statements on the effectiveness and advocacy of the broader use of biometrics to combat international terrorism. Interest in detecting the 'needle in the haystack' of terrorists intensified, as did funding for facial recognition projects, and FERET became a commonly used benchmark of this model. From this point on, as Crawford (2021, p. 105) argues, biometric systems expanded in scale and ambition. The terrorist attacks were the "turning point" for research into machine learning algorithms, especially those that make use of biometrics such as facial recognition and prediction, broadening the scope and use of these technologies for more general control and surveillance and not just for law enforcement (CRAWFORD, 2021). We also observed this dynamic in the previous chapter.

[35] International Biometrics is the leading international trade group representing the identification technology industry.

As the scale expanded, more data was needed to develop biometric algorithms. After all, the maxim that the more data, the better the intelligence took shape and became possible. One of the pioneering and largest image databases open and available for access by researchers and engineers wishing to test, develop, and refine facial recognition algorithms is the NIST Special Database 32 – Multiple Encounter Dataset (MEDS)[36]. NIST created MEDS to help the FBI and partner organizations refine tools, techniques, and procedures for facial recognition, as it supports what has become known as Next Generation Identification (NGI): forensic comparison, training, and analysis, as well as facial image compliance and interagency exchange standards[37]. In short, MEDS is a test database organized from an extract of photo presentations of deceased persons and their encounters with the criminal justice system through 'mug shots.'

Mug shots are photographs taken at the time of arrest, but in MEDS, they are used to train algorithms. These photos are from a fixed perspective and in good lighting, which is only possible in a standardized and controlled environment. The photos are all represented in the same way and act as indispensable data points for refining machine learning algorithms; the more data, the more refined they become. The inclusion of these images in the NIST database, according to Crawford (2021), has changed its meaning from being used to identify individuals in law enforcement systems to becoming the technical baseline for testing commercial and academic facial recognition algorithms. When mug shots are used as training data for facial recognition algorithms, they no longer function as identification tools in the criminal justice system. However, more broadly, they adjust and train an automated form of "vision" that will operate both in using these algorithms for law enforcement and not only. It should also be pointed out that these photos are used without any consent and are presented to the facial recognition algorithms in a decontextualized way, i.e., whether these people have been charged, arrested, or acquitted. What matters to the algorithm is the biometric data and its legibility.

The MEDS dataset has become a substrate for comparing algorithmic accuracy. In collaboration with the Intelligence Advanced Research Projects

[36] Available on: https://www.govinfo.gov/content/pkg/CHRG-107shrg81678/html/CHRG-107shrg81678.htm . Accessed: November 30, 2023.
[37] Available on: https://www.nist.gov/itl/iad/image-group/special-database-32-multiple-encounter-dataset-meds . Accessed on: December 23, 2023.

Activity (IARPA), NIST has organized competitions with these photos in which researchers compete to see which algorithm is the fastest and most accurate[38]. As Crawford (2021, p. 93) argues, the NIST databases foreshadow the emergence of a logic that now permeates the technology sector: the belief that everything is data and is there to be extracted, no matter the photograph's context. We can observe this extraction being normalized by developers and the tech industry (as I will see in more detail in the analysis of Clearview AI in chapter 4): the data is available to be used with little or no questioning of its underlying collection and production policy.

Here, I reinforce that the training and reference data set and their collection and use practices do not exist per se (RUPERT et al., 2013, p.29) but are produced in 'sticky' trajectories (KAUFMANN et al., 2019). Personal, social, and political meanings are not perceived and/or "neutralized" when data is recomposed, reused, or decontextualized. The image becomes part of a mass of aggregated data, part of a broader system that teaches the machine to see, perceive, and recognize an anomaly. Although the algorithm is important in data processing, the data plays an important role in the conditions of possibility of what the algorithms can recognize.

As we have seen in this section, there is a continuity with some previous biometric methods that also used feature pattern recognition in (photographic) data, but with the difference that today, there is much more data available. The readability of biometric data and its translation into patterns by and through computer vision is important for the analyses proposed in this dissertation because it makes something or someone perceivable and actionable, at the limit being identified or not, recognized or not. In this sense, bringing something into the field of vision is not only a visual question of recognition but also a question of producing knowledge, that is, deducing and/or disturbing a certain sense of reality. As Foucault (2007, p.20) argues, visibility can be understood as an effort to make reality cognizable and make something visible to knowledge and governable.

Explorations of facial biometric data through algorithmic methods and techniques have proliferated and gained disciplinary legitimacy and competitions such as those run by NIST and even sponsored by players in the technology

[38] Available on: https://www.nist.gov/programs-projects/face-challenges . Accessed on December 23.

industry, such as Microsoft and Facebook. With its ability to overcome the visual as quantitative, computer vision through algorithms represents the technological benefit that Galton lacked. Although the eugenics project has long since lost its credibility, especially after the horrors of the Second World War, what Rose (2000) calls biocriminology still seems to be present in academia and institutional practices. According to Maguire (2009, p.15), rather than the 'success of revolutionary theories,' it is the 'absence of common theoretical acceptance or justification' that has become the mechanism by which many physiognomic experiments continue to be developed and re-adapted through the use of computer technologies.

The development of facial recognition and pattern recognition technology is deeply entangled with the controversial history of eugenics. This connection extends beyond the analysis of biometric data for identification and authentication. It delves into how these methods are used to classify, segregate, and control populations, thereby materializing practices of (in)security and violence. While most facial recognition systems claim to identify individuals, the most contentious ones openly profess to recognize 'types of people', echoing Galton's proposal. There are controversial instances where machine learning algorithms are used to predict sexuality[39] and propensity to crime[40] through facial recognition of images and videos, resembling the idea of identifying 'types of people' by segmenting the population into clusters and fixing them in historically stabilized categories.

It is important to note that the results of deep learning algorithms are different from previous methods, as we observed in chapter 2, which usually rely on identity categories that are known and relatively stable beforehand. The parameters algorithms can generate dynamically based on data that are malleable and relational, which favors effectiveness over fixity (CHENEY-LIPPOLD, 2017, p.6); however, generally, these parameters and clauses generated by the algorithm are "translated" into familiar categories (KOTLIAR, 2020). Here is the thing about machine learning algorithms: their results are taken as 'ground truth,' and stabilized

[39] WANG, Yilun; KOSINSKI, Michal. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of personality and social psychology, v. 114, n. 2, p. 246, 2018.
[40] FUSSELL, S. An Algorithm That “Predicts” Criminality Based on a Face Sparks a Furor. Available at: https://www.wired.com/story/algorithm-predicts-criminality-based-face-sparks-furor/ . Accessed on: May 20, 2024.

classifications are applied to a fluid complexity – a continuous flow of data, parameters, and feature production and grouping.

The analysis of biometric pattern recognition through algorithms exposes the very emergence and materialization of machine learning algorithms (CRAWFORD, 2021; AMOORE, 2020). At the end of this research, I hope to raise questions and paths that will allow us to take seriously how machine learning algorithms normalize a way of telling the truth, relating and ordering a multitude of things, with sometimes unpredictable consequences in the creation and legitimization of imaginaries and norms that are difficult to challenge. The notion that these technologies can produce evidence about something or someone reflects, among other things, the construction of discourses and public perceptions of what science and technology, crime, and justice are.

3.3. A “good enough” solution: facial recognition in security practices

Biometric data fused with algorithms are central to contemporary governance and security practices. There is a construction and circulation of knowledge about biometrics by a transnational field of security professionals, brought together both through professional practices and publications by international and technical-scientific organizations (PUGLIESE, 2012). The 'biometric ideal' is often shared by security professionals from the Global North and South (PUGLIESE, 2012; JAIN; ROSS, 2015; GATES, 2011). The routine use of these technologies has been understood as an essential element in realizing the security management paradigm in an optimized, objective, and efficient way to deal with the challenge of indeterminate and diffuse threats.

Biometric technologies, their proponents suggest, are almost impossible to mislead because unique identification symbols frame the information extracted from our bodies. Biometric data takes the form of both tracking who you are and telling a definitive story about who you are. As we have seen, the translation of people into data has historically operated with specific notions of the construction of categories of people and forms of suspicion, creating modes of representation and possibilities for action (HACKING, 2006, p.166). The possibility of action, in

this sense, is closely linked to the models of perception, recognition, and description of attributes embedded in our biometric data and the ability to process them.

As I have emphasized in this dissertation, the increase in confidence in the processing of biometric data by algorithms is part of a more general shift towards the naturalization of algorithms as tools and arbiters in various social and institutional practices with the promise of bringing reliability and objectivity to decision-making amid uncertainty (AMOORE, 2013). The distinct value and practical benefits of using biometric data are increasingly recognized, including in policing approaches, cross-border challenges in surveillance and intelligence gathering, and judicial, evidentiary, and forensic use. This trend of expanding the use of this data is also reflected in regulatory efforts to produce "best practices," such as that of the United Nations Security Council through resolution 2396[41], which requires states to develop and implement systems to collect biometric data to "responsibly and appropriately identify terrorists."

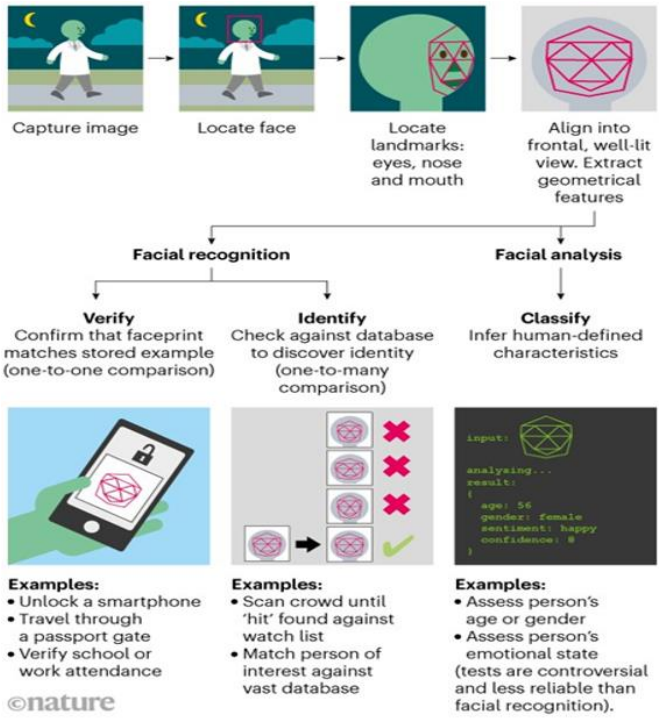
However, widely used biometric technologies anchored in a discourse of optimizing security practices, such as facial recognition technologies (FRT), are also the most debated for their errors and failures (ARADAU; BLANKE, 2021). As I pointed in section 2.3, more recently, facial recognition has become possible at scale through advances in machine learning; this widespread deployment has led to public debates and controversies about the errors and disparities that have resulted in prejudice and discrimination against certain social groups (BUOLAMWINI; GEBRU, 2018). There is much debate about using facial recognition and possible measures to mitigate errors and even limit its use in security practices, especially in policing.

Within the context of security practices, this section specifically addresses the utilization of automated facial recognition algorithms. The operation of FRT involves the fusion of facial images of an individual with a face database, followed by a comparison of facial feature patterns (such as eyes, nose, mouth, etc.). This process encompasses three fundamental steps: face detection (identifying a face in the image), face capture, and face matching with a database (determining the

[41] UNITED NATIONS SECURITY COUNCIL. Resolution 2396. Disponível em: http://unscr.com/en/resolutions/doc/2396 . Acessado em: dezembro de 2021.

identity of the face). Furthermore, facial recognition algorithms can be integrated with digital videos and images from closed-circuit television (CCTV), phone metadata, and internet history to construct a comprehensive profile of an individual's movements and lifestyle (SMITH et al. 2018). The figure below provides a visual representation of the typical functioning of contemporary FRT, highlighting its potential implications in security practices.

Figure 6. How facial recognition works



Source: CASTELVECCHI, 2020.

The larger the volumes of data available, the more familiar it becomes to use it in new ways and the ability to integrate biometrics and other data and metadata. Although it is a less precise technology than other forms of biometric identification (such as fingerprint scanning), it does not require direct contact with individuals, which makes it easier to implement. This "less invasive" form allows it to be used in public spaces for large-scale surveillance without those being scrutinized necessarily being aware of it. Security agencies have seen increasing the possibility of surveillance and identification on a "subtle" scale as one of the main benefits of using this technology.

In general, FRT operates in the search for identification and produces evidence about someone's identity (are you who you say you are? Who are you?).

However, it does not provide an absolute match of identity but rather a probable and parameterized identification, i.e., through a likelihood ratio. According to Goriunova (2019, p.20), the problem with the face as biometric data to be automated by algorithms is that it confuses probabilistic statistical techniques (machine learning) and the idea of unique data (biometrics). In other words, there is an ontological contradiction between the promise of "uniqueness" in facial recognition and the statistical calculation that generates facial models based on a training process involving thousands or millions of data. Machine learning algorithms do not operate based on a pre-defined model that links a facial image to a unique identity; they use statistical calculations to extract patterns from the data sets on which they have been trained to identify degrees of similarity probability.

Thus, FRT is in a constant process of modulation, and this perspective requires a new theoretical approach that takes into account the "inferential potential" and the "experimental procedure" that characterizes machine learning processes (PARISI, 2016, p. 472). Therefore, what happens when these statistical probabilities are interpreted as a definitive certainty about someone's identity in security practices? The issue is compounded as the data on which the probabilities are based recurrently reflect race and gender biases. An essential issue with FRTs, therefore, arises. On the one hand, these technologies are still linked to the idea that the face is a mechanism for individualization. On the other hand, using TRF at scale is made possible by machine learning algorithms that no longer rely on a direct link between the face and individuality.

A substantial portion of the current discourse on FRT revolves around the efficacy of these technologies, their impact on privacy, discrimination, and the biases they embody (FERGUNSON, 2017; BOULAWINI; GEBRU, 2018; BROWNE, 2020; TANWAR, 2019), and the crucial need for transparency in their operations, particularly when employed in security practices (ANANNY, 2016; HANNA-MOFAT, 2019). Error rates and false positives[42] have significantly influenced public discussions and the implementation of facial recognition algorithms.

[42] The false positives occurs when the machine mistakenly identifies the searched face as that of a person registered in the database.

It should be noted that FRT is used experimentally in practice. Algorithms used by security professionals do not have to undergo public or independent testing to determine accuracy, probability of error, or check for bias before being deployed. The distance between the testing processes of these technologies and their application becomes almost non-existent in practice.

As Aradau and Blanke (2021) argue, from laboratory testing to scientific, judicial, and human error, the errors and biometric technologies' scientific epistemology and development have been historically intertwined, as I analyzed in the previous sections. In other words, failures and errors are part of the tangle that makes these technologies possible to materialize and circulate in different spaces of experimentation. According to Pugliese (2010, p.44), from anthropometric methods to contemporary biometric technologies, their promotion is anchored in the argument that it is possible to eliminate subjective biases through the technical-scientific method. In this sense, errors, failures, and biases have been tracked, neutralized, or litigated from the perspective of the possibility of optimizing these technologies.

The error, as I have observed in this thesis is an integral part of the mode of truth enunciation pursued by machine learning algorithms trained in an ethos of constant optimization, in which error is acceptable and even desirable for learning. This view of error as productive is often complex and cannot be reconciled with approaches in the public debate about errors to eradicate them (ARADAU; BLANKE, 2021). Amid the widespread contemporary political desire to incorporate FRTs as anchors for optimized decisions in the criminal justice system, it is always worth noting that they are experimental arrangements that operate on probabilities and not certainties. The optimized algorithmic decision is not about precision, but a sufficient correlation (CRAWFORD, 2021, p.204).

If FRTs learn to see, perceive, and recognize, would this vision be completely objective, or would it incorporate particular ways of seeing? As we saw in the previous sections, technologies are not developed in a social vacuum; they are entangled in data and human and non-human practices. Machine learning algorithms incorporate a 'recognition regime' that identifies who or what matters to the event (AMOORE, 2020); they operate by assigning meanings to certain bodies from a disembodied gaze (BROWNE, 2015). More specifically, biometric

technologies, of which facial recognition is a part, are inscribed in racializing processes that make some bodies problematic and others not. Therefore, using facial recognition technologies is hazardous in contexts where certain groups are historically surveilled and policed.

That is why it is important here to look at how facial recognition algorithms, and more broadly machine learning algorithms, create the conditions for establishing who can be recognized and how to identify them. They make someone perceptible and available for the senses and action. Facial recognition algorithms make "what matters" in a given scene among a volume of data visible to the analyst precisely to reduce and level a field of vision. And whether someone is recognized depends on what the algorithm has been exposed to in the data. Since the machine learning algorithm adjusts the thresholds and weights, for example, through its exposure to the data. Therefore, FRT, by condensing what is essential, determine the possible "radicalized," 'risk," "criminal," and "illegal," infer trajectories and make security professionals' practices possible and recursively adjustable. While these algorithms work with probabilities, they also advocate a malleability and management of expectations in action in the present.

In addition, another question that we opened up in chapter 2, and which we move on to here, and which will be better explored in chapters 4 and 5, is how, despite errors and controversies about accuracy and bias, these technologies continue to be used in security practices and circulate in different contexts. It reinforces the understanding that algorithmic reason and its regime of truth are modulable and that logic of adjustment and optimization. The error does not limit the use of FRT; instead, it helps to increase the broader digitization of domains of everyday life, demanding the expansion of available data to improve accuracy, as we observed in section 3.2. We can see that there is a circular pattern of problematization. If the facial recognition algorithm (optimized solution) makes a mistake, this mistake is part of the process of optimizing the algorithm and improving its accuracy. In this sense, the error is not a problem but part of the solution for which the algorithm offers an "optimized" version.

In this chapter, I also highlight that the error is not a 'bug,' but part of the very way of reinforcing the epistemic authority of the TRF as a reliable technical-scientific apparatus that makes visible what a security "target" and what is not from

biometric data understood as unique. The TRF does not need to be perfect. It needs to be good enough to be implemented. In this sense, the strength of machine learning algorithms comes from the ability to make useful inferences, abstractions, and experimentations with vast patterns and even larger data sets that generate a possibility of action. The accuracy of the technology is not necessarily related to whether or not it is validated; rather than having high levels of precision (being "perfect"), the technology needs to be sufficiently efficient and useful in relation to the expected results, and these results end up reinforcing an inscription of political and social practices and asymmetrical power relations in an unequal distribution of (in)security. Some individuals and groups often become the object of attention and have their fundamental rights violated.

Finally, biometric algorithms, such as those for facial recognition, do not emerge or develop and operate in isolation. These technologies operate as recursively adaptive processes of varying the boundary between possibility and reality and as an apparatus for understanding reality itself. As analyzed, this is a central issue in the use of facial recognition algorithms in security practices, which are not the most accurate but are ‘good enough’. This is because they generate a contingent probability of an absolute decision (for example, recognized/unrecognized). As Crawford (2021) and Amoore (2020) argue, we need to be much more skeptical of claims that increasingly accurate and optimized ways are needed to frame and solve our social problems, especially security ones.

Part II

The entanglements practices of (in)security

4.
Clearview AI: “Building a secure world one face at a time”

> *Advanced AI to make us safer and more secure — wherever we live, learn, work, travel, or commerce.*
>
> Cleraview AI.

Clearview AI is a US startup founded in 2017 by Ton-That and Richard Schwartz[43] and backed by investments from Peter Thiel (also a Facebook investor and owner of security technology company Palantir) and from the Kirenaga Partners fund. The startup has been operating in the ecosystem of algorithmic facial recognition technologies that are becoming both an ignition for the practices of security professionals (from the police to the military) and evidence support in the context of criminal evidentiary proceedings. The promise of building a safer world through artificial intelligence, specifically through its facial recognition algorithm, is presented by Clearview AI on its website and social networks. As it states on the first page of its official website, the company's mission is “simple and impactful”: to drastically reduce crime and make communities safer. This promise is not as simple as it sounds, and offering a unique tool capable of making it possible is attractive. As we have seen in this dissertation, algorithms and what has come to be called artificial intelligence have been entangled in a discourse that frames them as efficient solutions for dealing with the uncertainty of persistent security problems.

Guided by Karen Barad's (2007) concept of “materiality”, the purpose of this chapter is to follow and analyze processes of materialization – the processes by which matter (heterogeneous entities) acquires meaning. For Barad, objects are dynamically produced through specific material-discursive practices and are open to re-articulation and remodeling. Inspired by Nick Seaver's (2017) algorithm research tactics, the proposal is to analyze the materialization process, various practices of the actors who try to stabilize the algorithm, which is contingent and can change; map the discursive representations; and trace the effects of algorithmic practices. This way, we can identify the socio-technical entanglement and imaginaries produced through algorithmic practices (BARAD, 2007; JASANOFF,

[43] Advisor to Rudolph W. Giuliani when he was mayor of New York.

2015). Here, I follow Latour's advice (2005, p.22) to let the actors define entities and trace the trajectory between their conflicting and controversial definitions.

As regards Clearview AI more specifically, this chapter aims at following this particular technology from its design to its institutionalized use in the practices of law enforcement agencies. Who is making these algorithms? What is the training data? What is the socio-technical context of the emergence/development of these algorithms? To what problem does it offer a solution? These are the first steps to mapping the infrastructure in which these technologies operate. In addition to that, I will look at the practices and spaces in which the algorithm has experimented, which are both fluctuating and dispersed in different contexts (the algorithm can be appropriated and transformed in various spaces, such as intelligence agencies, police departments, and courts). The idea is to stay and work through these complex chains of algorithmic observations to recognize the many writers of a single system. Therefore, they intra-act “beyond the moment of their inscriptions” (AMOORE, 2020) after their configurations in laboratories and tests with developers. The algorithm leads us to reflect on the relationships between (dis)united humans and non-humans, as well as digital and analog objects that participate in calculation processes. This distributed governance of algorithms places the researcher before the "non-closure" and "excess" of algorithmic contexts.

To do that, this chapter is divided into four main analytical movements. First, I explore the regimes of justification that made the emergence of the Clearview AI algorithm possible, particularly what problems this technology seeks to solve and what its promises are. In the second movement, I analyze the socio-technical context of its emergence and the multitude of practices that have made Clearview AI a sufficiently efficient security solution. Here, I am interested in technical attributes such as design, training data, the database, and how it works, but also social and political relations: who is funding it, who operates it, and how it operates. After all, the algorithm and its programming activities, scientific rationalities, and material constraints constitute a particular production context. The social and cultural spaces where algorithms have agency are shaped, ordered, and generated by algorithms themselves (DAHLMAN et al. 2021, p.4). In other words, following Barad (2003), the focus will shift from questions of correspondence between descriptions and reality to questions of practices, doings, and actions.

The third movement has as its nodal point the mapping of the field of disputes around the uses of the Clearview AI algorithm, as well as its criticisms and controversies. These frictions can be productive and ambivalent. On the one hand, they can lead to more precise reactions to the expansion of these technologies while allowing for them to be perfected. On the other hand, it makes them more adherent in multiple contexts. It is in this sense that I end the chapter with an analysis of how Clearview AI has reshaped and "optimized" its algorithm and expanded its use, even amid controversy. The expansion of modes of practice and contexts also operates in the sense of articulating credentials through narratives and arguments perceived as reliable and legitimate for 'assembling credibility' (ARADAU; HUYSMANS, 2019). I will look at how credibility is 'assembled' through a fluid, dispersed, contested, and open process of socio-technical practices rather than a fixed feature of the Clearview AI algorithm.

In this chapter, I am inspired by the question posed by Malte Ziewitz (2017, p.2): "What would it take to understand algorithms not as technoscientific artifacts but as a figure mobilized by professionals and analysts alike?" As noted in chapter 2, the writing of algorithms operates through various characters and in various dispersed spaces, from the laboratory to the street, the police station, the border, and the court. Therefore, following Clearview AI allows us to reflect on the effects of the discursive authority attributed to algorithms, their growing use by security professionals, and how this knowledge has circulated. The research interest is not in the specific configuration of a particular algorithm at a moment in time but in the practices, they make possible and are part of. For this reason, I will carefully analyze how Clearview AI has been framed as "building a secure world one face at a time." In other words, the more data you have and the better your facial recognition algorithm, the better and safer the world will be.

4.1. A search engine for faces

> *Clearview is basically a search engine for faces, so anyone in law enforcement can upload a face to the system and it finds any other publicly available material that matches that particular face.*
> Hoan Ton-That, 2020[44].

[44] In an interview on CNN Business with Donie O'Sullivan recorded on February 5, 2020. Available at: https://www.youtube.com/watch?v=q-1bR3P9RAw (00:20). Accessed on August 5, 2023.

> *Clearview AI is dedicated to innovating and providing the most cutting-edge technology to law enforcement to investigate crimes, enhance public safety and provide justice to victims*.
>
> Clearview AI[45]

Clearview AI is an "innovative" facial recognition algorithm capable of identifying a person from a single input provided, and show other public photos (HIll, 2020). After collecting images of people's faces from the Internet, the algorithm converts all facial images into vectors. When a user uploads a photo to the app, it matches all photos with similar face vectors. The application then returns to the screen user links to publicly available images on the Internet, which usually include additional information about the identified person[46].

"So, this is what it looks like. It's like Google for faces. Instead of typing in words or text you upload a photo"[47]. The comparison of Clearview AI's technology with Google is a recurring one: of the 15 publicly available video or audio interviews used in this research, in six, CEO Ton-That explains his technology as a search engine, like "Google," only for faces available to security forces. The comparison with one of the world's most used internet search engines is not random. It is one of the ways of 'presenting' the company's tool as powerful and 'disruptive,' as it is reinforced in the marketing material, and at the same time, easy to understand, use, and follow current legislation.

The start-up received much attention and emerged from the 'shadows' in January 2020, when the New York Times published *"The secret company that could end privacy as we know it"* (HILL, 2020). This report spotlighted not only the start-up but also its business model: its algorithm, the way it extracts data, and the way it is marketed. Before this, Clearview AI deliberately worked in silence while offering its product to law enforcement agencies in several countries and private security companies. In 2019, more than 600 police agencies in the United States already used the tool (HILL, 2020). It was already offered to 2,900

[45] Available at: https://app.hubspot.com/documents/6595819/view/640216868?accessId=a02cbe. Accessed on August 5, 2023.
[46] ACLU v. Clearview AI, Inc., No. 2020 CH 04353, 1. https://www.aclu.org/legal-document/exhibit-2-signed-settlement-agreement . Accessed on August 5, 2023.
[47] Interview with Hoan Ton-That at the AI4 2021 event on August 17, 2021. Available at https://www.youtube.com/watch?v=LyPV_IISNCw (8:40). Accessed on August 5, 2023.

organizations in 2019, including private companies and public institutions such as the US Border Protection and immigration agencies, the FBI, the Secret Service, and Interpol (HASKINS; MAC; MCDONALD, 2020). Just 18 months after the publication of the New York Times article, Clearview AI was named one of Time magazine's "100 Most Influential Companies" in 2021 (PEARSE, 2021). Self-described as "the world's largest facial network."

Although security agencies worldwide have used different facial recognition technologies for some time, Clearview's algorithm goes far beyond traditional technologies, as noted in chapter 3. The great 'innovation' brought about by the company's software is the vast database of over 30 billion photographs scraped from websites worldwide. It is no exaggeration that journalist Kashmir Hill's recent book on the company's history is titled *Your Face Belongs to Us: A Secretive Startup's Quest to End Privacy as We Know It* (2023). Even if a person has never heard of Clearview, it is likely that if they have any online presence or if they are in a photo taken by a third party (even if in the background of the photo) and posted, for example, on Linkedin or Facebook, it probably means that they are in the company's database. In this way, whether or not we have consented to our faces appearing in the photos, many become training data and the composition of the database itself. It is important to note that much of our data is freely available for use when we post it online, without the typical safeguards found in physical infrastructures. So, it is profoundly challenging to discern who is using it and for what purposes.

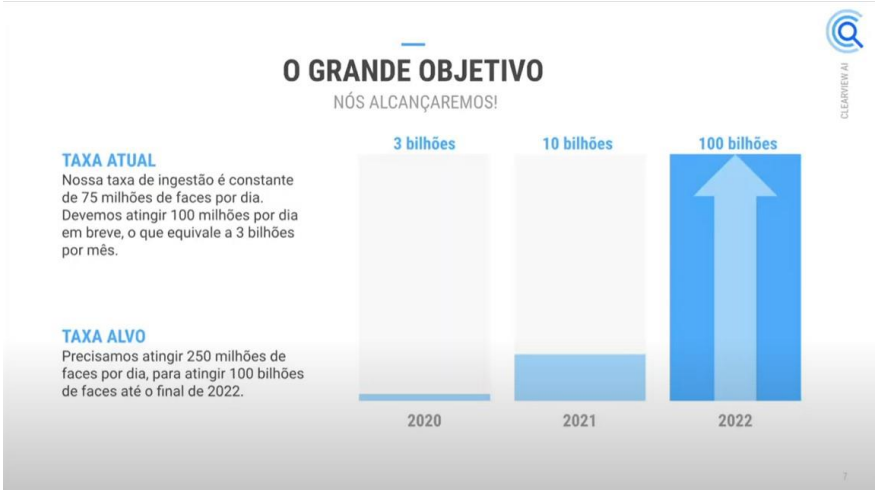
At the panel sponsored by the North American start-up at ISC Brasil 2022[48] and attended by its CEO Thon-Tat, sales representative Ramiro Valderrama declared that the company's "goal is to have at least 100 billion images available in our database without loss of quality in a few years". At a prospecting hearing for the company with the Brazilian Ministry of Justice held on February 9, 2022, by Copaq[49] – a committee made up of representatives from each of the units and sectors

[48] The panel sponsored by Clearview AI at ISC Brasil 2022 took place in auditorium 1 on September 21, 2022. The panel was formed by Edmir Tardero, Luiz Ortiz and Ramiro Valderrama Aramayo.

[49] This commission was created in 2019 to establish partnerships between public and private companies or institutions with the aim of innovations, technological solutions, and best practices to promote and foster the modernization and re-equipment of public security bodies (BRASIL, 2019). The Ministry of Justice's Copaq meetings are open to all of those agencies who have interest in learning more about the object of discussion. However, the testing and procurement of contracts do not need to be intermediated by the federal government. In other words, procurement takes place autonomously in each agency without standardization or regulation.

of the National Secretariat for Public Security (SENASP). The company's sales representative reaffirmed the company's goal of expanding the database even further as "the big goal." As we shall see, what Clearview's algorithm does and its ability to do it depends on its database, not only to produce more specific results in security agents' "searches" but also to refine its algorithmic model.

Figure 7. A slide showing the company's capacity, growth, and objectives



Source: 5th Copaq/SENASP public prospecting hearing, via the Access to Information Act[50]

In addition to its vast database, the company considers[51] that its solutions are from other existing facial recognition tools, with its database not confined to any jurisdiction, capable of identifying not only people previously arrested or in the suspect database, but anyone with any online presence[52]. Therefore, the company claims that Clearview AI is able to provide "results" at consistently high rates of accuracy across all types of demographic group"[53]. In addition to allowing "agencies to gain intelligence and break down simple and complex crime," Clearview is a platform with:

> user-friendly compliance features, including a comprehensive intake form and strong administrative oversight (...) offers

[50] The hearing is available upon request through the Access to Information Act, Process No. 08198.023803/2022-21.
[51] The document titled "Clearview AI: Leads, Insights, and Relationships" is available here: https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92. Accessed on August 5, 2023.
[52] Ibid.
[53] CLEARVIEW AI. HJ48 Study: The Future of Facial Recognition Technology. [Comments Submitted]. Economic Affairs Interim Committee's Panel Discussion, February 9, 2022, 11:30-Noon MST. Available at: https://app.hubspot.com/documents/6595819/view/293634780?accessId=6f984c . Accessed on August 5, 2023.

> increased accountability and transparency within jurisdiction. Our platform generates high-quality results with speed and accuracy, when searching for post-event investigative leads. Additionally, agencies have the ability to import their own private, customizes facial datasets to have a comprehensive, unified platform for identity management. This further enhances the power of Clearview AI's facial network[54].

To understand the conditions of possibility for Clearview AI to emerge as an essential security solutions company "for solving crimes and preparing court cases"[55] and how it managed to have "the largest database in the world by far" (CLEARVIEW AI, n/d), we need to move a few steps back and analyze the company's materialization processes and its algorithm.

Clearview AI has been dynamically produced through specific material-discursive practices, humans, machines, data, failures, and other 'interferences' open to re-articulation and remodeling. Beyond a static arrangement or development in a linear trajectory, intra-actions emerge and also (re)configure themselves. According to Barad (2007), it is through these specific agential intra-actions that the properties that make the phenomena are determined, and materialized concepts acquire meaning. In other words, the meaning of the algorithm is not isolated but part of a multitude of practices and actors, its tangled organizational configuration.

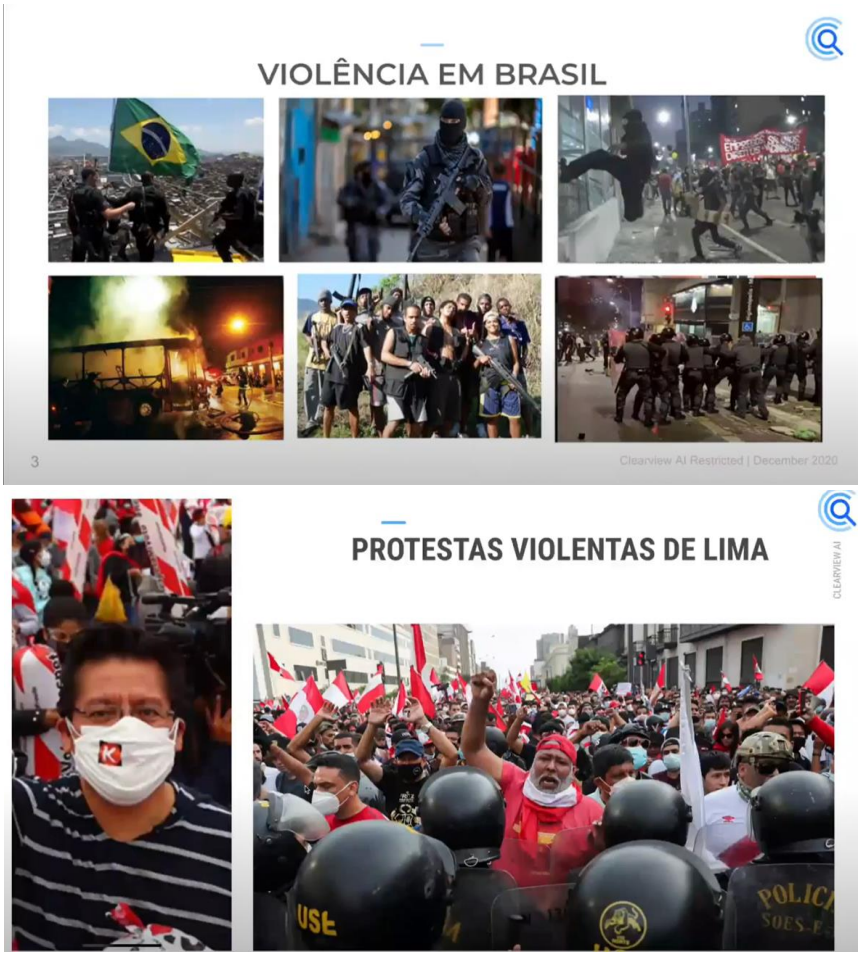
Considering the corporate discourse (documents, marketing materials, interviews, and website), the composition of the advisory board[56] (all names linked to US security agencies), and the technologies that are being developed and where they are being tested, the problem for which Clearview AI's algorithms are a "revolutionary tool" is security. For Ramiro Valderrama, the idea is to "combat the emerging threat of crime using the public internet". According to the "Company Overview"[57] document, the tool is being used to investigate various types of cases

[54] Ibid.
[55] CLEARVIEW AI. Clearview AI Company Overview https://app.hubspot.com/documents/6595819/view/640216868?accessId=a02cbe . Accessed on August 5, 2023.

[56] Available at: https://www.clearview.ai/press-room/clearview-ai-announces-formation-of-advisory-board . Accessed on August 5, 2023.
[57] Available at: https://app.hubspot.com/documents/6595819/view/640216868?accessId=a02cbe . Accessed on August 5, 2023.
[57] Ibid.

around the world: violent crime, drug trafficking, organized crime, fraud, theft, terrorism, missing persons, human trafficking, sexual crimes against children, violent protests, among others. It is also used by different agencies, from local police to particular services[58]. The slides below, presented at a meeting with Copaq/SENASP[59] held on April 13, 2022, exemplify how the company seeks to offer its technology as a solution to various security threats.

Figure 8. Slides showing the company's understanding of Latin America's security problems



Source: Presentation of the latest version of Clearview 2.0 to COPAQ/ SENASP, via the Access to Information Act.

By researching the history of the development of the technology and the company, it is noteworthy that this problematization was not always clear: initially, the idea was to create a "google for faces", and not to promote a "safer" world, but to be used for some purpose in which searching for faces and finding them would

[58] Ibid.
[59] Acces to Information Act's Process nº 08198.034501/2022-55.

be useful, capital-generating and legal (HILL, 2023). Our faces are crucial for linking accumulated digital data, our digital traces that tell us about our daily lives and relationships. This is valuable not only for security authorities, but also for companies, advertisers, journalists and others. This is an important element for my analysis: first the algorithm and the data scraping method were built and then it was defined where it would be used and for what purpose.

Before it was called Clearview AI, the company was known as Smartcheckr LLC, founded in 2016. Smartcheckr's emergence is associated with far-right conservative circles in US politics (O'BRIEN, 2020). The software was first used at the Deplora Ball event held at the National Press Club in Washington, DC, on the night of January 19, 2017, to celebrate Donald Trump's victory and inauguration so that anti-fascists could not enter the event. This information was revealed in a document presented to the Hungarian government, offering an algorithm as a solution to "identify people affiliated with the Open Society Foundation"[60]. Furthermore, there was a non-formal adaptive use of the algorithm that could be purchased through the Apple store as a 'secret toy of the rich,' which customers used at parties and events to identify people[61].

Moreover, Smartcheckr presented itself to political candidates as a consulting firm to build "voter profiles," "opposition research," and "micro-segmentation" through its photo-finding tool in "unconventional databases" (O'BRIEN, 2020). It did not succeed in occupying this space in the market, however. For Hill (2023, p. 120), the facial recognition software was not ready at that time, and it did not find any interested parties for the tool. In 2016, the political market for the use of personal data scraped from social networks was poignant, as became evident with the Cambridge Analytica case (ANNA-VERENA NOSTHOFF; MASCHEWSKI, 2017), when data was extracted without consent to

[60] Exposing the secretive company at the forefront of facial recognition technology. Available at: https://www.npr.org/2023/09/28/1202310781/exposing-the-secretive-company-at-the-forefront-of-facial-recognition-technology . Accessed on August 5, 2023.
[61] Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich (Published 2020). https://www.nytimes.com/2020/03/05/technology/clearview-investors.html. Accessed on August 5, 2023.

create behavioral profiles, make predictions, and influence voter behavior in the 2016 US presidential election.

Smartcheckr had a tool but not yet a target audience or a specific objective. Clearview AI as we know it emerges in a context of centralizing the facial recognition algorithm, improving it, and expanding the database to be a security solution, initially for private companies (HILL, 2023, p.166). In 2018, Clearview AI's database grew from 20 million to 1 billion photos in less than a year – an expansion intended to achieve greater accuracy, thereby differentiating the company in the security technologies market (HEILWEIL, 2020). In order to develop and run the algorithm and amass a vast database, a suitable infrastructure was needed to enable development, implementation, and practical use, such as a combination of powerful servers with high-performance graphics processing units (GPU), storage, and cloud computing. In this sense, the initial investment, the "bet" by Peter Thiel and the investment company Kirena Partners was what guaranteed the operationalization of the first version of what is now known as the Clearview AI algorithm (HILL, 2023; TRACXN, n/d).

Clearview AI's emergence as a security start-up required a profound contrast to its previous form, especially in attracting clients and investors (O'BRIEN, 2020). As O'Brien (2020) describes, there was a move towards professionalization and a focus on what the technology could do. Also, the company distanced itself from political controversies and "negative" associations (HILL, 2023, p. 120) – reason why there was an effort to "erase" the former traces of the company's formation, including de-indexing information about Smartcheckr's existence in Google searches (O'BRIEN, 2020). As part of its remodeling, the company established relations with Greg Besson, Lieutenant Commander of Detectives of the NYPD Cyber Task Force of the FBI-NYPD. The rapprochement with security professionals was so meaningful for the company's redirection that Clearview AI offered an unpaid demo to the NYPD in 2018[62]. Besson presented the tool to Chief

[62] For its use, the NYPD and Clearview AI entered into a confidentiality agreement, suggested by the police department and not by the company (HILL, 2023, p.170). Therefore, in the interviews collected and the company's statements, there is a denial of this test by the NYPD. However, it is possible to see this relationship with the company's emails and prospecting documents and materials. The point was that at the time, in 2018, there had already been a critical debate about the use of facial recognition technologies, and the NYPD needed to protect itself from the legitimacy of the test (HILL, 2023).

inspector Chris Flanagan, who was interested in what the tool could do to optimize investigations. Here, it is worth noting that the NYPD is one of the largest police departments in the US and has an important role in the circulation of police practices worldwide, such as the digitization process and CompStat's[63] managerialism (SMITH; BRATTON, 2001). In this sense, the support of William Bratton and the implementation of the CompStat system were essential to scale up the pilot project at the NYPD in 2018 (HILL, 2023, p.166; HASKINS, 2021). Within a few days, some NYPD officers were using Clearview daily, especially Financial Crimes Task Force, Grand Theft Division, Facial Identification Section, and a Department of Homeland Security task force (HASKINS, 2021).

Clearview's promotional materials claim that the company "began solving crimes using newly developed facial recognition technology" in 2018 (O'BRIEN, 2020). The NYPD laboratory also operated as a space for testing and producing reports that quantified the use of software and the number of searches and uses for prospecting other clients. As we observed in previous chapters, the prototypical use of algorithms in security practices has become standard practice as an opportunity to experiment, learn, and optimize these technologies. Moreover, if the algorithm fails, it would need more practical experimentation. According to Aradau and Blanke (2022), the algorithm combines performative effects even when it does not seem to work. The NYPD was a gateway to the law enforcement market and soon Clearview AI was signing paid contracts with police departments in the states of Indiana, Florida, and Tennessee.

Currently, Clearview users stretch from the FBI, the Customs and Border Protection (CBP), Interpol, and hundreds of regional, state, and municipal police departments in US. Clearview AI sought to create a global biometric identification system for security purposes that would cover the public and private sectors (MAC; HASKINS; MCDONALD, 2020). According to the document obtained by BuzzFeed News, people associated with 2,228 law enforcement agencies, companies, and institutions collectively created accounts and conducted nearly 500,000 searches – all of which were tracked and recorded by the company in 2019

[63] CompStat is a crime data management system that the NYPD developed in the 1990s that uses crime data to identify problematic areas ("hot spots") and target resources accordingly to reduce crime.

(MAC; HASKINS; MCDONALD, 2020). At the same time, there is no clear line that restricts to law enforcement agencies the sale, use, or testing of this biometric tool, which points to how the company's discourse about the scope of its tools has been shifting.

To gain new customers, Clearview offered access not only to organizations but also to individuals within them, sometimes with limited supervision or even without the awareness of their superiors. Thus, the company circulated among various agencies without being formally sanctioned for use through free trials, which only required an institutional email address. The 30-day free trials for police officers operated as a way to showcase the tool's capabilities and get officers to encourage their departments to purchase and praise the tool by focusing on its efficiency in "identifying criminals" to officers from other police departments at conferences and online (MAC; HASKINS; MCDONALD, 2020; HILL, 2023). The free testing of officers using police departments or government email addresses has created situations where law enforcement agencies sometimes seem to lack "clarity" that their employees are using the tool. In this process, we see individual professional discretion without clear organizational accountability protocols or training.

The practical uses of Clearview have also raised issues of protocols needing adaptations to meet law enforcement requirements. Among those updates aimed at increasing the control over tools such as facial recognition technologies, there was the possibility of identifying searches with the case number or the ID of the person using the system. Also, there was the concern that the tool followed law enforcement parameters of privacy, purpose, and proportionality (HILL, 2023). Clearview's code of conduct states that individual users should be "authorized by their employer" to use the tool, but this seemed to be more of a guiding principle than an enforceable rule (MAC; HASKINS; MCDONALD, 2020). The adaptability of both the algorithm and its interface is one of the features singled out as a Clearview differential, as described in the presentation of the latest version of Clearview 2.0 to SENASP, Brazil.

Tests at the NYPD in 2018 indicate that the algorithm had a 50% hit rate (HILL, 2023. p.171), a far cry from the almost 98% that the company achieved in

the NIST tests of 2021 and 2023[64].The low accuracy required an optimization of the algorithm and an expansion of the database to increase the possibility of "matches" in the searches made with the software. "The Internet was an ocean of faces, and they had caught some of the fish available" (HILL, 2023, p.171). The internet was the essential tool for optimization of Clearview's algorithm. The Internet is a surveillance system that contains and tracks data. In this sense, it is impossible to connect to the Internet, let alone participate in social networks, without participating in data surveillance, whether as an individual citizen or a group (ZUBOFF, 2019). It is difficult to have a presence in the internet and do not have one single photo, and the different photos of the same person are essential for the development of accuracy of FRT.

The technical development of the algorithm was key to its stabilization in the security technology market, as well as to consolidate its use among security agencies as an "efficient and race-neutral technical alternative"[65]. Even when the Clearview algorithm was operating experimentally, and without an accuracy calibration, it was already being acquired and increasingly used. In an email to the NYPD with "tips" sent by Clearview in 2019, the company replied that it is adding hundreds of millions of faces every day and for people to make several attempts each week, you may be able to find a match in a few weeks, even if you cannot right now (HASKINS, 2021). In other words, Clearview AI was not perfect, but its identification was seen as accurate enough, better than previous forms of recognition centered on human expertise. As Ton-That said in an interview, "With sufficient training data, accuracy can surpass that of human eyes."[66] Access to the most extensive and structured set of data is the way to build and refine learning models that group and target the patterns of a population (THYSTRUP; HANSEN; AMOORE, 2022).

---

[64] Available at: https://pages.nist.gov/frvt/html/frvt11.html and https://app.hubspot.com/documents/6595819/view/449537243?accessId=b92ab6. Accessed on August 5, 2023. In the following sections we will analyze the development of the algorithm and its way of optimizing through errors and failure.

[65] MEMORANDU de August 14, 2019. Legal Implications of Clearview Technology. https://s3.documentcloud.org/documents/6668315/Atlanta-Facial-Recognition-ORA.pdf Accessed on August 5, 2023.

[66] Ton-That in an interview with Amanpour and Company on February 19, 2020. Available at: https://www.youtube.com/watch?app=desktop&v=GeIc-yhGmx4 (1:50). Accessed on June 15, 2023.

Furthermore, by stating that Clearview AI is neither designed nor intended to be used as a single-source identity system[67], the security agent "needs to analyze the images."[68] The biometric tool shows lead insights and expose unknown relationships and associations that support technical decision-making and increase case clearance rates[69]. It puts the agent in the decision-making loop, thus also decentralizing responsibility for specific decisions and possible false positives[70]. Thus, as we can see, there is an interweaving of agency procedures, software usage protocols, objects, people, and algorithms. Amid this multitude and complexity, opacity and calls for more transparency have proliferated.

On March 6, 2019, Clearview's testing period was terminated. Emails obtained by Buzzfeed indicate that the NYPD did not sign a paid contract with Clearview AI after these 90 days trial, mostly out of fear that the technology was "morally problematic" concerning privacy (HILL, 2023, p. 171). Several officers seemed to like the tool, nonetheless (HASKINS, 2021). In March 2019, for instance, Detective Michael Furia of the facial recognition unit declared he would "do everything I can to help the NYPD sign with Clearview because I am a big supporter" (HASKINS, 2021). Regardless of official support, many NYPD officers continued to use the algorithm until at least February 26, 2020 (HASKINS, 2021). In an interview, an NYPD spokesperson in 2020 said that "established practices have neither authorized the use of services like Clearview AI nor expressly prohibited it" (MAC; HASKINS; MCDONALD, 2020).

Indeed, the gray zone resulting from the absence of regulations specific to facial recognition technologies use has been an advantage for the circulation of these tools among security professionals. However, the criticisms and controversies already being raised in the public debate could be a problem for the rising company to attract customers[71]. In order to guarantee the protocols and legality of the use of

[67] MEMORANDU de August 14, 2019. Legal Implications of Clearview Technology. Available at: https://s3.documentcloud.org/documents/6668315/Atlanta-Facial-Recognition-ORA.pdf . Accessed on August 5, 2023.
[68] Ibid.
[69]CLEARVIEW AI: leads, insights and relationship. Accessed at: https://app.hubspot.com/documents/6595819/view/454213344?accessId=50f575. Accessed on August 5, 2023.
[70] I will describe the algorithm-human relationship in more detail in the next section.
[71] It is noteworthy that the critical debate on the use of facial recognition, also linked to movements for privacy and civil liberties, gained momentum in 2018. San Francisco, for instance, became, in

the software, Clearview recruited Paul Clement, the former attorney general of the United States, as its lawyer to guarantee the legitimacy of operations for prospective clients. He provided legal cover for the police to circumvent civil rights concerns, writing protocols and communiqués claiming that Clearview did not violate the privacy of those who had already voluntarily posted their images and content on social media. Hence the discourse that the "unconventional" database was just a way to make information that already existed easy to find, a "Google for faces."

> We conclude, based on our understanding of the product, that law enforcement agencies do not violate the federal Constitution or relevant existing state biometric and privacy laws when using Clearview for its intended purpose. (...) face recognition technology promotes constitutional values in a manner superior to many traditional identification techniques and competing technologies[72].

Although there is no specific federal legislation on facial recognition tools in the US, Illinois has developed regulations about the corporate use of biometric data, and some cities have banned the technology altogether. In this regulatory vacuum, Clearview has thrived, distributing free trials and encouraging law enforcement agents and authorities to invite their colleagues and do as many searches as possible. "Using is the best way to test technology thoroughly. You never know when a search will find a match" (HASKINS; MAC; MCDONALD, 2020). According to official emails published by Buzzfeed, the company set a goal of 100 searches per week using the software in 2019 at the police department in Appleton, Wisconsin (HASKINS; MAC; MCDONALD, 2020). Clearview AI has also encouraged authorities to test its facial recognition algorithm in unusual situations, such as identifying corpses.

The circulation of knowledge about Clearview's recognition capacity and its alleged effectiveness (mainly due to the extensive database) in the circles of experts and security professionals was essential for marketing and expanding the use of the algorithm. The maxim of doing more with fewer resources in a more technical way, while being "simple" to use, permeates the company's presentations and marketing

2019, the first US city to ban the use of facial recognition software by police and other government agencies.

[72] MEMORANDU de August 14, 2019. Legal Implications of Clearview Technology. Accessed at: https://s3.documentcloud.org/documents/6668315/Atlanta-Facial-Recognition-ORA.pdf .

documents. "In less than a second, it [Clearview] can find a match in our database of millions of photos. It can be integrated into security cameras, iPhone/iPad apps, and with an API,"[73] said the company's abstract for a security technology event for the retail market in 2019.

By mid-2020, more than 2,400 police agencies in the United States were using the software (GARVIE, 2019). In 2019, the company offered the trial to agencies and companies in 26 countries outside the USA, including Australia, Belgium, Brazil, Canada, Denmark, Finland, France, India, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Norway, Portugal, Saudi Arabia, Serbia, Slovenia, Spain, Sweden, Switzerland, the United Arab Emirates, and the United Kingdom (MAC; HASKINS; MCDONALD, 2020). At the 2019 edition of the ISS World North America, former Clearview CEO Richard Schwartz gave a talk titled "How Intelligence + Image Recognition Can Save a Risk-Prone World" and also participated in the panel "Best Practices for Deploying a Facial Recognition Program."[74]

The worldwide organization of sworn police officers, the Fraternal Order of Police (FOP)[75], owns the FOPConnections platform, which was used to send emails advertising Clearview to its members. Clearview sponsored features in Police Magazine on facial recognition and was invited to present its services on two panels at a security conference, according to an email from the conference organizers obtained by Freddy Martinez, policy analyst at Open the Government[76]. The startup has also placed ads on CrimeDex[77], a platform for financial crime investigators. In an interview with the New York Times (2020), Sgt. Nick Ferrara of Gainesville, Florida, stated that he learned about the software through CrimeDex and considered Clearview's application to be superior to the one provided by the FBI (FACES) (MAC; HASKINS; MCDONALD, 2020) because it does not require "perfect photos" (i.e., people looking directly into the camera).

---

[73] Available at: https://onezero.medium.com/this-is-the-ad-clearview-ai-used-to-sell-your-face-to-police-8997c2a6f0a8. Accessed on August 5, 2023.
[74] Vision 2029 - Total Store Expo. Available at: https://web.archive.org/web/20180927124945/http:/tse.nacds.org/plan/vision-2029 . Accessed on: 8 Nov. 2023.
[75] Available at: https://fop.net/. Accessed on: 8 Nov. 2023.
[76] Ibid.
[77] Available at: https://www.crimedex.com/ Accessed on: 8 Nov. 2023.

Figure 9. Clearview AI marketing Documents Delivered to Atlanta Police Department

Source: MAC; HASKINS; MCDONALD, 2020.

One of the central US immigration control agencies, Immigration and Customs Enforcement (ICE), was added to the software's client list in 2019. Clearview has also been used within the Department of Justice, where the list of government organizations testing the company's facial recognition software includes various offices in the FBI (5,700 searches in at least 20 different field offices), the US Secret Service (around 5,600 searches), the Bureau of Alcohol, Tobacco, Firearms and Explosives (over 2,100 searches); and the Drug Enforcement Administration (around 2,000 searches).

It is not only about law enforcement, however. Clearview has also licensed the application to a few private companies for security purposes, such as Gavin de Becker and Associates and SilverSeal. Indeed, for a company that currently keeps its focus on law enforcement tools, Clearview's list of former clients includes a surprising number of private companies in sectors such as entertainment (Madison Square Garden and Eventbrite), gaming (Las Vegas Sands and Pechanga Resort Casino), sports (NBA) and even cryptocurrency (Coinbase).

Clearview's "success stories" include testimonials from agencies that have solved dead-end cases and identified murderers and child sex offenders – the latter being a recurrent figure in “success stories”. As we have seen, several state agencies place their trust in the capacity of sophisticated facial recognition algorithms to

optimize their practices, as illustrated by the marketing material Clearview AI provided to the Atlanta Police Department:

> Clearview's speed and accuracy are unsurpassed (...) Clearview puts the world's most advanced facial recognition technology and largest image database in your hands, allowing you to turn a photograph into a solid lead in an instant (MAC; HASKINS; MCDONALD, 2020).

In its presentation material to Copaq/ SENASP of Brazil's Ministry of Justice and Public Security, I also find the testimony from Jason Webb of the Oxford, Alabama Police Department and FBI expert in the field of counter-terrorism, who points out that:

> In the counter-terrorism field, its experience in identifying people is close to 100%. I think this is partly due to the database, as well as the emphasis he places on instructing this preparation work in the research image. This increases the chances of a positive return[78].

In addition to that, Clearview is celebrated as a suitable technology for surveillance, given that it is "silent" – it operates passively in the background, unnoticed by the surveilled subjects (INTRONA; WOOD, 2004). In a statement from the Clifton Police Department in New Jersey, officers were attracted to using Clearview's technology partly because of its ability to search individuals in the "field" without reporting them to a court[79].

The algorithm spread "virally" (HILL, 2023, p.173), as we could see in this section. In a relative short time, span, the company became a significant global player in facial recognition technology, especially for an audience the application was not expected to serve at first: law enforcement agencies. As we noted in chapters 2 and 3, security problems have been increasingly framed as uncertain, and facial recognition algorithms operate in an ecosystem of algorithmic technologies that aim at making security practices more efficient in dealing with phenomena understood as “social disorders”, such as violent protests, crime and terrorism. The next section turns to the political force of the discourse on objectivity and efficiency of which Clearview AI is an expression. In doing so, I am interested in exploring

[78] 5th COPAQ/SENASP public prospecting hearing, via the Access to Information Act. Process no. 08198.023803/2022-21.
[79] Available at: https://cdn.muckrock.com/foia_files/2019/12/05/OPRA_1311.PDF . Accessed on: 8 Nov. 2023.

the terms under which Clearview's high efficiency has come to be claimed as superior to human discretionary judgement to solve complex problems, especially in the security domain. My purpose is to understand how its emergence as a "model" for making security practices more efficient is connected to the expansion of the horizons within which "possible suspects" are claimed.

4.2. Face makes cases: "Revolutionary face recognition platform"[80]

> *We have created a technology that is way more accurate than anything before it's better than the human eye.*
>
> Hoan Ton-That, CEO da Clearview AI, 2020[81]

> *World's best facial-recognition technology combined with the world's largest database of headshots. Stop Searching. Start solving*.
>
> Clearview AI, n/d.

In advertisements, websites, official reports, audiences, interviews, fairs, and events, Clearview AI's facial recognition algorithm and its database are always presented as superlatively positive resources, not only because of their alleged high technical and technological capacity, but also because no solution available in the market is similar. Observing the conditions of possibility for the Clearview AI algorithm to emerge as the "state-of-the-art"[82] is relevant because there is a politics in how algorithms are created, used, and imagined (AMOORE, 2020; SEAVER, 2017; CRAWFORD, 2021).

In the previous section, I looked at the conditions of possibility for the company's emergence. As I have pointed, the materialization of Clearview AI has not been a linear process, but one full of pauses, re-articulations, and remodeling resulting from experimentation and practical uses. In this section, the proposal is to observe the circumstances in which the Clearview AI algorithm is produced and constantly adjusts and changes depending on the system in which it is inserted.

---

[80] https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92

[81] Em entrevista para o podcast "This week in start ups" on April 25, 2020. https://www.youtube.com/watch?v=wNLK_f6m4e0&t=44s (24:16). Acesso em 05 de agosto de 2023.

[82] CLEARVIEW AI. HJ48 Study: The Future of Facial Recognition Technology. [Comments Submitted]. Economic Affairs Interim Committee's Panel Discussion, February 9, 2022, 11:30-Noon MST. Available at: https://app.hubspot.com/documents/6595819/view/293634780?accessId=6f984c.

Therefore, it is necessary to carefully and critically observe how the algorithm "folds and unfolds" data, methods, technology, social actors, and organizations (LEE et al., 2019). Attention to the work in between or in the production of input flows to an output that will be the ignition point for a security action. Many hands materialize it, and this multiple authorship is codes, data, sharing, and practices incorporated into different workflows that combine fragments into products through human work (AMOORE, 2020). These data collection, cleaning, and processing workflows are distributed and circulated globally and are essential in the condition possibility of a “Revolutionary face recognition platform.”

The open-source software movement and the circulation of knowledge about algorithms in a freely available form were central to the development of the Clearview AI algorithm (HILL, 2023). Transparency and reproducibility are increasingly important aspects of computer science research, and the release of open-source repositories containing code, data, and documentation is now a standard practice. Indeed, the collaborative development of open-source software has come to be a privileged site for the scientific community to negotiate meanings, establish norms, and build knowledge. Training sets and the socialization of codes in collective writing are essential elements in establishing the epistemic boundaries that govern the functioning of algorithmic systems. Moreover, they are essential for understanding socially significant issues related to these systems (CRAWFORD; PAGLEN, 2021), such as levels of accuracy and biases concerning specific demographic groups.

In this context, the interaction and acquisition of data and code from platforms such as Github (a social networking site where programmers can share their work), image databases such as Open Face and MegaFace, and the archives of academic work by engineers and computer scientists published on arXiv.org and other publicly available repositories have been the basis for a period of exponential progress in machine learning techniques and methods (LUNCHS; APPRICH, BROERSMA, 2023). Other engineers read about their techniques, find ways to improve them, and then publish articles about their improvements, which generally provide a sense of “moving forward” in the field. It is through this 'virtuous cycle' of multiple actors in distributed code writing that facial recognition techniques and other machine learning techniques have been developed and improved. This open-

source mode of development created the conditions for Clearview AI, which was able to capitalize even from the sludge outside the cycle (HILL, 2023, p.102-103). In an interview, Ton-That said: "I could not have figured it all out from scratch, but these other guys, like Geoff Hinton[83], they stuck with it, and it was like a snowball" (HILL, 2023, p.103).

The sharing of data between computer scientists, engineers, and programmers from university laboratories to Silicon Valley offices paved the way for Clearview and the development of other algorithms, methodologies, and techniques for using artificial intelligence. The emergence of the company's development intersected with this crucial moment in the development of AI in general, as we saw in chapter 2: the development of hardware, new data storage techniques, cloud computing, and the massive amount of data available with the popularization of the internet and social networks. As a result of these processes, advances in neural network research and computer vision techniques, such as facial recognition, have become more scalable and accurate (CRAWFORD, 2021; MACQUILLAN, 2019).

The first version of the algorithm, still in the former Smartcheckr LLC company, was developed by Ton-That and physicist Terence Liu. In a "geek curiosity" interview, they point out that the objective was to build a biometric algorithm that used a methodology of scraping data from the internet, i.e., a training database that was able to expand beyond existing repositories (HILL, 2023). As noted in the previous section, the aim was to create a "google for faces", for the ever-expanding training database also meant the expansion of the possibilities for the use of biometric facial recognition (HILL, 2023). To this end, instead of hiring a development team, the first people recruited to work at Clearview AI were

[83] Hinton is referred to as the “godfather of AI”. He is particularly famous for his work on the development of deep learning algorithms, which have played a key role in the evolution of modern artificial intelligence. He was one of the first researchers to demonstrate the effective use of neural networks for machine learning tasks and is the co-inventor of the "backpropagation" and "divergent contrast" algorithms, both of which are crucial for training deep neural networks. Recently, he has expressed growing concerns regarding the proliferation of misinformation, the potential impact of artificial intelligence on the job market, and the existential risks associated with the development of artificial intelligence. Available at: https://www.theguardian.com/technology/2023/may/02/geoffrey-hinton-godfather-of-ai-quits-google-warns-dangers-of-machine-learning . Accessed on 13 nov. 2023.

"freelance coders adept at web scraping" to "hunt faces on the internet" (HILL, 2023, p.128). The aim was to have a large database that stood out in the growing biometric market and could also be a differentiating factor when training its facial recognition algorithm. By the end of 2018, the company had collected one billion faces from the internet.

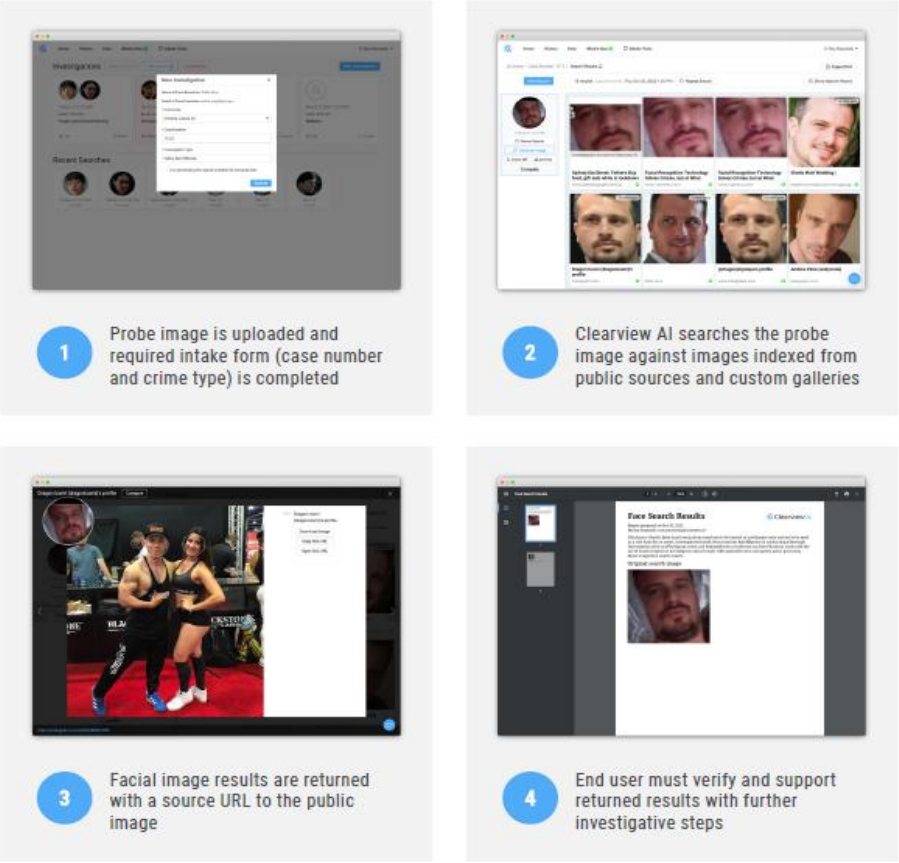
Even though the use of such database has changed over time, and the company itself has changed its name and sector, what we see is the constant reuse of data (which was not initially generated to train and feed this technology) and of the algorithm (optimization of methodologies and techniques already published and of the Smartcheckr version itself). In machine learning data, reuse is key because it allows the generative use and application of partial knowledge (parameters, clusters, and patterns) to unknown situations; it is decomposed and reappears in different contexts (THYLSTRUP, 2019). Importantly, the idea of reuse advances a logic that facilitates generalization to new problems based on tangled fragments of data (THYLSTRUP; HANSEN; AMOORE, 2022). It is precisely this adaptability and "transfer learning" that allows its use as an "optimal solution" for multiple social problems (GOODFELLOW et al., 2016, p. 527). Thus, algorithms thus modify themselves in and through their continuous, iteractive and recursive relationships with input data, creating conditions for the possibility of future worlds and practices (AMOORE, 2020).

The algorithm

Clearview engineers have developed software that automatically collects photos of people from various websites. The software generates metadata such as time, date, and location of the images and can provide direct links to social media profiles. According to the company[84], their software works in four stages in the user interface, as shown in the figure below.

Figure 10. "How it works"

[84] Available at: https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92.



Source: Clearview AI, Company Overview

Here, we can see the entanglement between the security agent and the algorithm through the interface. The user enters a photo and creates its classifications (for instance, the case number and the type of crime), as well as being able to create and label galleries in which searches can be saved[85]. We can also see that there is a requirement for a complete description of the production and recording of data in the apparatus (BARAD, 2007). By adding these fields to the interface, a story is told – that is, the circumstance of the data production – by the person responsible for the recording. At the same time, there is an initial motivation, a suspicion that ignites the search for biometric data for identification and investigation.

In addition, this process produces statistics and quantifies the practice of agents and technology, allowing searches to be "auditable"[86] by supervisors – who could be the head of a police agency, for example. Although the algorithm is "the best in the world at facial recognition," the company's document reveals that the output generated by the neural network has in its pipeline the final analysis of the

[85] Ibid.
[86] Available at: https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92.

security agent in confirming the identity (as seen in Figure 10). In the end, the professional can write feedback on the search by adding a comment in a text box or clicking the "thumbs up" icon[87]. As the company presented on its stand at the LAAD Defense & Security 2023[88], interaction with users is also a way of optimizing the software to meet the specific demands of each agency and country. In other words, there is an adaptative feature and a possibility of "customization" to each organization and country, as Ramiro Valderrama reinforced in the two presentations here analyzed and the presentation given at ISC Brasil 2022[89].

"A Clearview AI search is the beginning, not the end, of an identification process."[90] According to the text published on the company's website, 'A Practitioner's Guide to the Responsible Use of Facial Recognition Technology',

> the algorithm does not automate decision-making but places the onus on a person to analyze the image search results and apply investigative best practices. Law enforcement still has to do the investigative work, but you gain a massive advantage in the form of investigative leads that take months or even years to uncover[91].

As we can see from the excerpt above, the discourse is that the technology does not replace the researcher's expertise but helps to increase the results' speed and accuracy. The expert discourse is fragmented between human and non-human practices and, at the same time, contributes to assembling credibility for the software by involving the human in the looping. This information does not appear in the documents related to the first uses of the algorithm in 2018 or 2019, but in 2020, when the company gained attention in the public debate, the insertion of

[87] 5th COPAQ/SENASP public prospecting hearing, via the Access to Information Act. Process no. 08198.023803/2022-21.
[88] LAAD Defense & Security (International Defense and Security Fair) took place in Rio de Janeiro between April 11 and 14, 2023. It is considered the largest and most important defense and security fair in Latin America. In its 13th edition, the event was attended by manufacturers and suppliers of weapons and technologies for the Armed Forces, Police, and Special Forces; military personnel from the Armed Forces; police forces from various institutions; government authorities - including foreign delegations - communication professionals and the academic community. Available at: https://www.laadexpo.com.br/ . Accessed on June 11, 2023.
[89] ISC Brasil is the Brazilian edition of the ISC Security Events - International Security Conference & Exhibitions brand. The fair was held between September 21, 2022 and September 23, 2022 at Expo Center Norte in São Paulo. Available at: https://www.iscbrasil.com.br/pt-br/o-evento.html. Accessed on June 14, 2023.
[90] Clearview AI Overview product. Disponível em: https://app.hubspot.com/documents/6595819/view/454213073?accessId=c85a92. Accessed on August 5, 2023.
[91] Professional's Guide to the Responsible Use of Facial Recognition Technology. Available at: https://www.clearview.ai/post/a-practitioner-s-guide-to-the-responsible-use-of-facial-recognition-technology. Accessed on: 10 Nov. 2023.

humans into the loop provided another layer of expertise and accountability amid criticism of possible misuse (HILL, 2023). More specifically, developing and incorporating "gatekeepers" into the system's interface offered a record of which agents are using it and for what purposes. As noted in the previous section, the reliability of security professionals regarding the legitimacy of the use of the company's software was and has been important for the circulation and adherence of the technology. In addition to that, the algorithm has been intra-actively remodeled and rearticulated through material-discursive practices.

Clearview's algorithm also works to "solve" a question I raised in chapter 2: the more data, the more actionable this volume can be for security professionals. The proposal is to operate as a tool to filter "information that is there, on the Internet,"[92] producing leads and insights. The manageable actions of security professionals by filtering a massive amount of operate data as an attempt to capture the "unknowns" and "anomalies" in order to maintain order (AMOORE, 2013). The best model for "connecting the dots" is to bring it to the surface of security agents' attention, making this anomaly known (AMOORE, 2013; 2019; 2020). It is at this point that Clearview can make this process more accurate, technical, fast, accessible ("easy-to-use" and developer-friendly) and mobile (CLEARVIEW, n/d). Mobility here means both being available for computers, mobile devices, and even smart glasses, and in terms of the range of spaces and practices in which the application can be used[93].

Clearview's algorithm is made up of a system of deep convolutional neural networks (CNNs), one of the machine learning techniques understood to be the most "successful" in the development of artificial intelligence (NEGRO; PONS, 2022). CNNs have significantly changed the state of the art of many computer vision applications, such as facial recognition (more on this in chapter 2). Artificial neural networks work 'similarly' to a biological brain, transmitting various signals to other neurons to map an image. At a 2019 hearing before the U.S. House Committee on Homeland Security examining government use of facial recognition, the director of the NIST, Dr. Charles Romine, stated that recent advances in facial

[92] Thon-that interview at CNN Business' with Donie O'Sullivan, March 6, 2020. Available at: https://www.youtube.com/watch?v=q-1bR3P9RAw (16:10).
[93] We will look at this in section 4.4.

recognition technologies were a "game-changer."[94] According to him, the increase in the "accuracy and capabilities of the systems we have seen in recent years" resulted from "the advent of convulsive neural networks and machine learning capabilities to do image analysis"[95]. Importantly, this does not mean that they are error-free, especially when used on poor-quality images and in adverse conditions. As discussed above, errors make the learning process that is key to the continuous optimization of algorithms.

The distinction of CNNs from traditional facial recognition technologies primarily lies in their approach to feature extraction. Before CNNs, feature extraction in facial recognition relied on linear extraction methods, focusing on points within an image. As in the case of the algorithms used by Clearview AI, CNNs transform images into mathematical formulas, or vectors, based on facial geometry, moving beyond mere point analysis. These embedding vectors representing faces possess unique properties, diverging from those derived in other general contexts. Notably, they have definitive labels of absolute truth: a face does or does not belong to a specific individual without ambiguity. In this sense, they differ from general computer vision tasks, where an object might belong to multiple conceptual categories; for instance, a "Siamese" can be classified as a "cat" and also an "animal."

Facial recognition algorithms aim to cluster vectors belonging to the same individual closely while keeping those of different individuals apart. The high-dimensional space in which these vectors exist displays a highly clustered statistical distribution, with the number of clusters being inherently limited by the finite number of people in the world. This advanced approach to facial recognition demonstrates significant advancements in terms of performance on unstructured data, generalization capabilities, and computational complexity for scalability, as outlined in Wen et al. (2016) and further detailed in the Clearview AI patent US 20220122356A1.

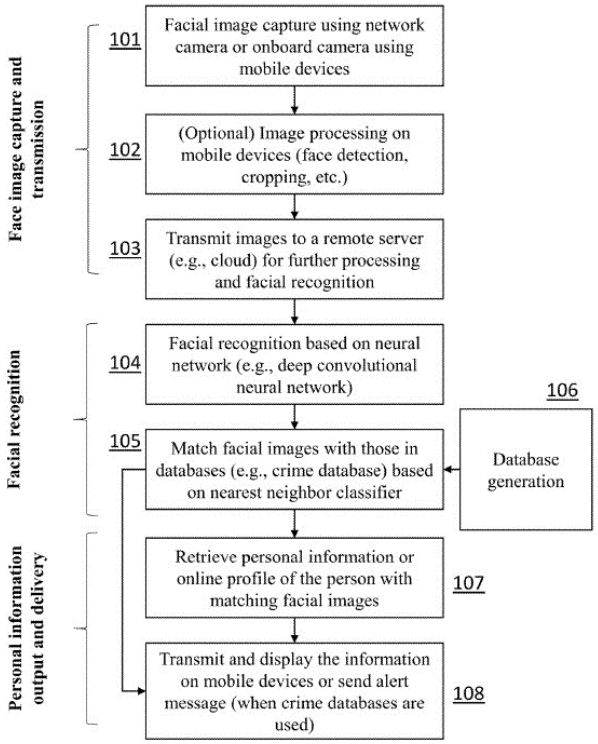
---

[94] FACIAL RECOGNITION TECHNOLOGY: PART II ENSURING TRANSPARENCY IN GOVERNMENT USE HEARING BEFORE THE COMMITTEE ON OVERSIGHT AND REFORM HOUSE OF REPRESENTATIVES ONE HUNDRED SIXTEENTH CONGRESS FIRST SESSION. [s.l: s.n.]. Available at: https://docs.house.gov/meetings/GO/GO00/20190604/109578/HHRG-116-GO00-Transcript-20190604.pdf . Accessed on November 8, 2023.

[95] Ibid.

With its vast data directory, Clearview AI's algorithm clusters all photos with similar vectors into "neighborhoods". The database consists of embedding vectors, and the matches are not literal or exact but based on similarity scores and a search limit, i.e., how close they are to the query vector (PATENT US 20220122356A1, 2022). The algorithm works on similarity correlations through probabilities of being or not being that person to whom the photo is being grouped. In this way, when a user uploads a photo of a face to the Clearview's system, it converts the face into a vector and then shows all the analyzed photos stored in the "neighborhood" of that vector, along with links to the websites where those images came from. In other words, in addition to detecting and recognizing the image, it is possible to extract metadata information from it, such as the location.

Figure 11. Clearview AI's facial recognition algorithm



Source: Patent US 20220122356A1 - Methods for providing information about a person based on facial recognition, 2022[96].

These steps, shown in Figure 11, demonstrate a general flow of how computer vision transforms images and videos into actionable knowledge. Images

[96] US20220122356A1 - Methods for providing information about a person based on facial recognition - Google Patents. https://patents.google.com/patent/US20220122356A1/en?q=(%22clearview+AI%22)&oq=%22clearview+AI%22&sort=new Accessed on August 5, 2023.

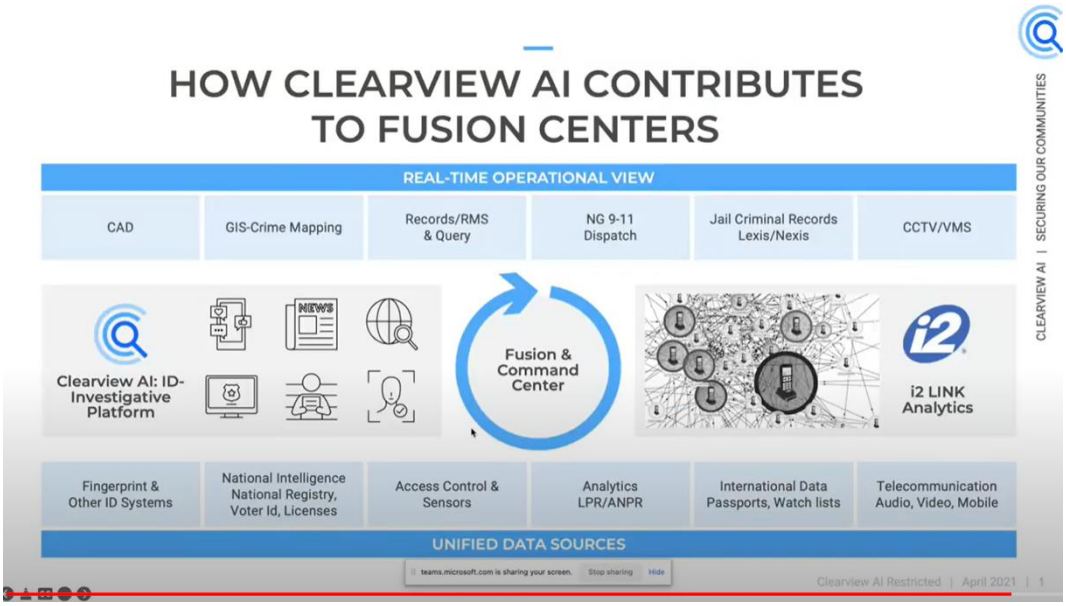
are mobilized to produce meaning. According to the company, "wholly *objective* and *technological* criteria[97] Clearview's algorithmic system operates as a tangled set of practices (human and non-human) that define parameters and filter the "reality" observed through images. These technologies make it clear to the analyst who the target is and other data that can be reused and shared with other algorithmic systems.

In the recordings of the presentations made by Copaq/ SENASP of the Ministry of Justice and Public Security of Brazil on April 13, 2022, the company representative reinforces the adaptability and compatibility of the software. According to him, “Clearview AI contributes to the fusion" of an ecosystem of algorithmic technologies used for security purposes, as represented in Figure 6. From real-time surveillance to pattern analysis algorithms with correlation visualization, such as i2 link Analytics, used by various intelligence agencies to "capture possible radicalized" networks of relationships in data and metadata (LIMA, 2020). One of the essential functions of algorithms like i2 link Analytics is to import data from various sets of databases and produce visualizations that will help reveal connections that would not otherwise be made (LIMA, 2020).

That confidence in algorithmic reason has been achieved by extracting, reading, and understanding pixels from digitized images as an objective way of producing knowledge both about the past as well as inferring about emerging behavior (SAUGMAN, 2020; CRAWFORD; PAGLEN, 2021). What Clearview is doing represents a "turning point" in which our faces would be indelibly linked to our online tracks, a link that would make it impossible to escape our past traces (HILL, 2023).

Figure 12. "How Clearview AI contributes to fusion"

[97] CLEARVIEW AI. Clearview AI Company Overview https://app.hubspot.com/documents/6595819/view/640216868?accessId=a02cbe, p.9. Accessed on August 5, 2023.



Source: Presentation of the latest version of Clearview 2.0 to Copaq/ SENASP, via the Access to Information Act.

Therefore, seeing does more than just showing things; it reconfigures practices (AMOORE, 2020) and confirms or transforms the distribution of positions (RANCIÈRE, 2021) of what is understood as the "best" practice of seeing and understanding security and also what the targets of (in)security are. As we can see, rendering and processing the image through algorithms allows for a different kind of knowledge production (AMOORE, 2020; SAUGMANN, 2020; ARADAU; BLANKE, 2022). However, during this moment of processing, data and algorithms collaborate in ways that humans cannot necessarily understand on the way to the output. This collaborative moment of dispersed data processing is difficult to reconstruct due to the capacity and speed of computational processing that machines exhibit at the user interface and even with their developers. This tangle of human and non-human practices affects not only the opportunities of those whose lives remain as residue in these piles of data but also all the other people whose data is incorporated into these moments. It matters which data is added to a data set, under what conditions, and according to what parameters. Furthermore, for what Clearview AI sets out to do, data is central.

The database

"The powerful matching software is only half of the technology story."[98] The company's differential in attracting investors and customers from the outset is its growing database of public photos from the Internet. Silicon Valley giants like Google and Facebook already have vast databases of people's photos, but they have not launched any biometric "search" tools. Clearview's approach to scraping data from the open Internet is highly controversial and considered problematic regarding privacy (REZENDE, 2020).

The context in which Clearview AI emerges was not the most attractive for the production of technology using social media data and facial recognition algorithms, especially given the growing controversy over facial recognition and a turn in the debate on privacy and surveillance following the Edward Snowden revelations (BIGO et al., 2015; HILL, 2023). For these reasons, Clearview was not considered as a viable application for Big Techs at that period[99]. One example is that in 2011, the then-president of Google said that it was the only technology the company would not develop because it could have harmful effects. In this sense, as Hill (2023, p.207) points out, Clearview's importance does not lie in its technical-scientific advance, but rather in the fact that the company's developers were willing to cross a line that other technology companies were not interested in crossing at the time.

The algorithm's ability to generalize and infer in the world, as noted in chapter 2, depends on its exposure to the world with a complex set of varieties, i.e. a wide distribution of different data examples (JACOBSEN, 2023). Leading computer vision researcher Kai-Fu Lee says that "AI is basically run-on data, the more data, the better the AI works, more brilliantly than how the researcher is working on the problem" (FRONTLINE, n/d). Few disagree with this logic. Data sets are an integral part of how a machine learning algorithm works. Without input, there is no output. Strangely, relatively little is known about the origins, contents, and end points of the image input used in computer vision, particularly facial

[98] MEMORANDU de August 14, 2019. Legal Implications of Clearview Technology. Available at: https://s3.documentcloud.org/documents/6668315/Atlanta-Facial-Recognition-ORA.pdf . Accessed on August 5, 2023.

[99] In his book, Kashmir Hill names the projects already under development by Facebook, now Meta, and which were discontinued due to their lack of "viability" (HILL, 2023, P. 128-136).

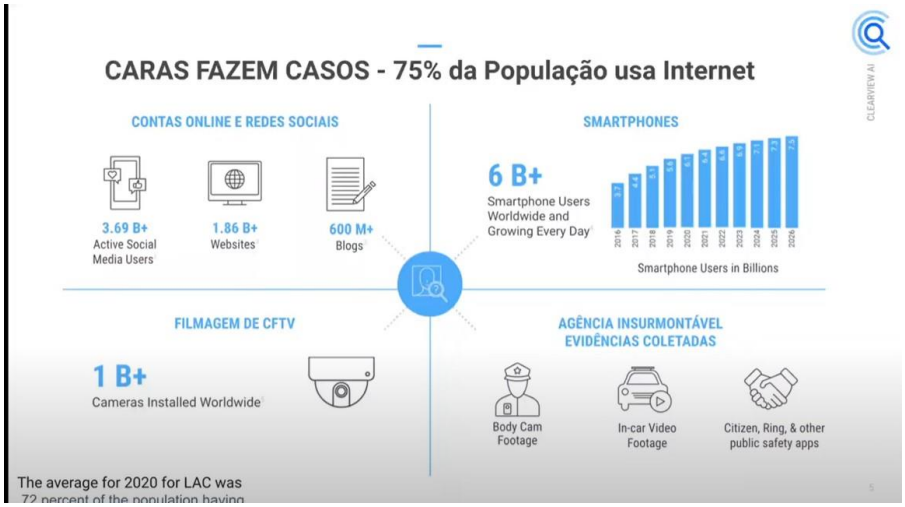
recognition. Researchers and developers have increasingly turned to the Internet as a primary data source to obtain vast amounts of data because it is scalable, fast, free, and legal. That is also the path Clearview AI has taken.

For developers of biometric technology, the word ‘selfie’ is the short version for biometric profile. “Today's selfie is tomorrow's biometric profile”[100]. The popular biometric industry website BiometricUpdate.com produced over 100 pages of biometric news results related to "selfies" from 2014. What was once seen as a form of personal expression on the Internet has been operationalized in security systems. As Harvey and La Place (2019) reinforce, a photo is no longer just a photo when it can also be surveillance training data, and data sets can no longer be separated from algorithm development when the algorithm is now built with this data. Following Barad (2007), that data does not pre-exist its use and reuse, but it is constituted through its entanglement in the broader “experimental arrangement”. With machine learning algorithms, these experimental arrangements encompass more-than-human environments, including computer scientists, data, GPU algorithms, human traces, wires, servers, and varied contexts.

According to the already mentioned prospecting presentations for Brazil's Ministry of Justice and Public Security, the exponential expansion of the use of the internet and social networks is framed as a tool for "combating threats"[101] – as shown in Figure 13, “faces make cases.” In addition to the bank of images publicly available on the internet, there is the possibility of establishing connections, weaving a thread between various biometric facial data by associating it with other applications and sensors to which security agencies have access, as shown in Figure 14. In its "Overview of Company" document, Clearview claims to offer a solution to the following problem: "How do law enforcement sift through this massive amount of digital evidence and synthesize it to help them solving more crimes?"

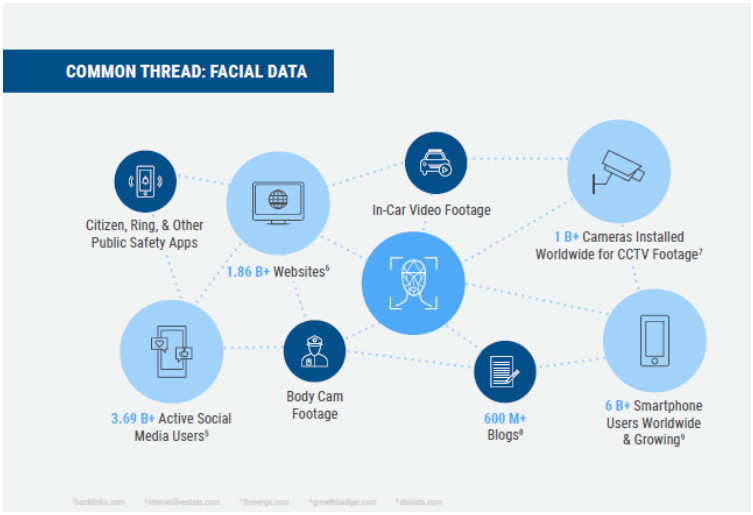
Figure 13. "Faces make cases"

[100] Today's selfie is tomorrow's biometric profile. Available at: <https://adam.harvey.studio/todays-selfie/>. Accessed on: July 12, 2023.
[101] Presentation of the latest version of Clearview 2.0 to Copaq/ SENASP, via the Access to Information Act. (15:45).



Source: Presentation of the latest version of Clearview 2.0 to Copaq/ SENASP, via the Access to Information Act.

Figure 14. Common thread: facial data



Source: Clearview AI, Company Overview

These data trails may seem insignificant on their own, but they become valuable when integrated with other data, offering infinite possibilities for analysis and growth (ARADAU; BLANKE, 2022, p. 35). No data point is too small to contribute to algorithmic knowledge and generate insights, enabling security professionals to find the proverbial needle in the haystack (ARADAU; BLANKE, 2022, p. 40).

According to the document sent by Clearview AI to the United States Office of Science and Technology Policy (OSTP) on January 15, 2022, the data available to the public on the Internet is valuable because, unlike traditional government databases, it can capture people who are not previously known to the authorities, i.e., who have not had an encounter with the criminal justice system. Here, as in

other documents produced by the company, Clearview AI reinforces how its technology creates conditions of possibility for broadening suspicion towards an emerging anomaly.

In addition, the multitude of constantly expanding data also enables the algorithm to have a high accuracy rate in different demographic groups and low-resolution photos (CLEARVIEW et al.). According to explanations provided in the presentation to Copaq/SENASP on April 13, 2022, the application's user interface offers an option to improve low-quality images ("flip, AI exposure, and AI blur"). Moreover, the algorithm is trained to recognize and identify a person of interest even amid facial occlusions (wearing a mask and glasses, for example), low-resolution images, and poor lighting. As noted in the previous chapters, facial recognition aims to find everyone in a crowd to collect all possible data to find a single "needle in a haystack," a searched face that is claimed to present a risk. The software will only find this "needle" by comparing its vectors with all the other faces' vectors and by producing modulations of norm and regularity, and probabilities of similarity and dissimilarity.

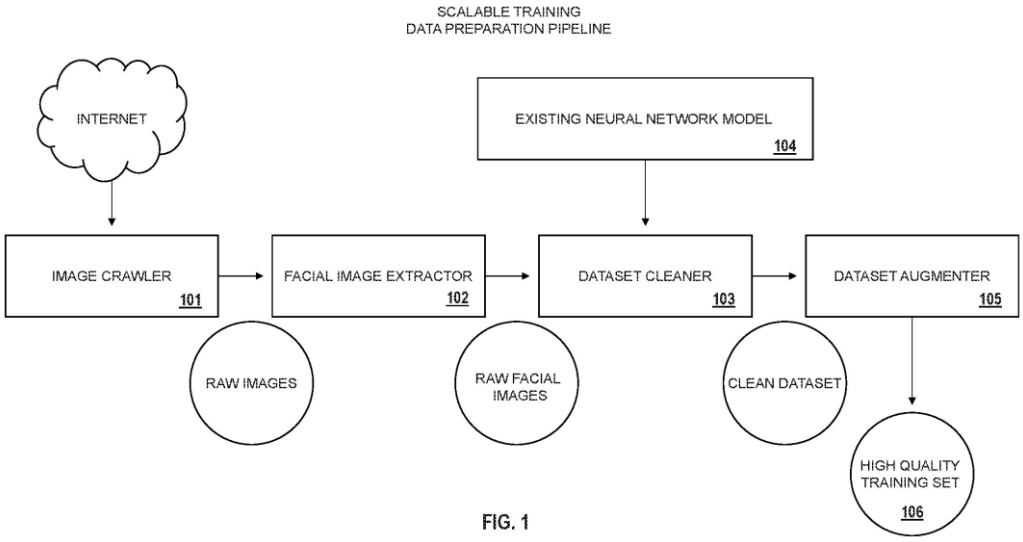
The centrality given to the volume of data also brings to light the work needed to manage this digital data. Data does not simply flow between public and private spaces and spheres; it must be made transportable, translatable, and transformable. These data infrastructures have come to permeate our daily lives; after all, it is through the increasing datification that the conditions of possibility are created for how the Clearview algorithm operates. Therefore, data needs to be understood as in it becoming something through various practices (BELLANOVA; FUSTER, 2019). Clearview's software can scan over a billion faces in less than a second[102]. Although the algorithm's capabilities are far beyond anything ever produced, the method of collecting facial images singles out the company's algorithm: "The true 'secret sauce' is data."[103]

[102] Presentation of the latest version of Clearview 2.0 to COPAQ/ SENASP, via the Access to Information Act.

[103] MEMORANDU de August 14, 2019. Legal Implications of Clearview Technology. p.10. Available at: https://s3.documentcloud.org/documents/6668315/Atlanta-Facial-Recognition-ORA.pdf . Accessed on August 5, 2023.

In 2022[104], Clearview acquired “Patent US11694477B1 – An efficient distributed trainer with gradient accumulation on sampled weight for deep neural networks in facial recognition”[105], a document that specifies the workflow of data scraped from millions of web pages that are prepared, cleaned, and optimized to refine and enrich data while minimizing the presence of noise, in addition to implementing a "highly efficient" distributed training method for deep neural networks that are employed in facial recognition[106]. Such method solves the “storage problem” resulting from the constantly growing database[107].

Figure 15. Data preparation pipeline



Source: Patent US11694477B1

Figure 15 shows the architecture and data processing capacity required for the Clearview AI software to function efficiently. The new architecture, made possible by the aforementioned patent, began to be implemented in 2021 and has made it possible to reduce computing costs by 80%, while also optimizing the transfer rate, allowing for more space so that more data can be added. According to

[104] At the time of writing this research, Clearview had three patents: i) "Scalable Training Data Preparation Pipeline And Efficient Distributed Trainer For Deep Neural Networks In Facial Recognition" (US No. 11,333,000). S Patent No. 11,443,553); ii) "Methods for Providing Information About a Person Based on Facial Recognition" (US Patent No. 11,250,226); and iii) Efficient Distributed Trainer with Gradient Accumulation on Sampled Weight for Deep Neural Network in Facial Recognition (US Patent No. 11,694,477).

[105] Available at: https://patents.google.com/patent/US11694477B1/en?q=(%22clearview+AI%22)&oq=%22clearview+AI%22&sort=new

[106] Ibid.

[107] Available on: https://www.clearview.ai/post/how-we-store-and-search-30-billion-faces. Accessed on August 5, 2023

Terese Liu, Vice President of Machine Learning and Research at Clearview, the method combined two open-source projects, Faiss and RocksDB[108], revealing the importance of open source for the company's technological development, as argued in the previous pages.

Although the company's technology is protected by corporate secrecy and its method is currently a patent – i.e., intellectual property – Clearview's system and its technical improvements throughout the years relied on public data and free access to information. At the same time, the language of patents reinforces a claim to knowledge, produces a metric of innovation "and leaves the door open to a cascade of new uses" (KARTZ, 2017, p.14). Indeed, patents transform ideas into a legal form of recognizable, defensible, consumable, and saleable property. Patents offer ways for us to envision socio-technical imaginaries that can be achieved through advances in science and technology (JASANOFF and KIM, 2015, p. 2). In the case of Clearview AI, patents, tests, and certifications provide legitimacy to the discourse that frames the algorithm as "highly accurate" and "without bias", as well as a revolutionary algorithm both in technical and practical terms, given its ability to solve complex problems.

The accuracy

The question that permeates how the rationality of machine learning algorithms operates is not one of accuracy but one of probabilistic correlation. However, accuracy rates are relevant for understanding the discursive struggle around the stabilization of technologies. As seen in chapter 3, although there is no consensus on standardization and accuracy, initiatives such as the tests carried out by NIST have provided developers, users of facial recognition technologies, and civil society with a layer of credibility and trust concerning the algorithms tested. Clearview has already undergone two NIST tests between 2021 and 2022. In the first occasion, the company was rated among the world's most accurate facial recognition companies. Clearview debuted as the best algorithm among American

[108]How We Store and Search 30 billion Faces. Disponível em: https://www.clearview.ai/post/how-we-store-and-search-30-billion-faces. It was accessed on November 02, 2023.

companies, placing it along the 'world's heavyweights,' including Japan's NEC and Russia's NtechLab[109].

The latest NIST tests confirmed that Clearview AI's algorithm correctly matched photos with an accuracy rate of 99.85 percent (12 million photo samples) and correctly matched VISA border photos with an accuracy rate of 99.86 percent (1.6 million photo samples). The tests confirmed the "superior" accuracy and reliability of Clearview AI as a facial recognition tool, particularly for law enforcement[110]. After being ranked first in the US in all categories of an individual test (1:1), Clearview AI reached the top positions in the one-to-many test (1:N). In the "in wild photos" (Rank-1), which measures the effectiveness of a facial recognition algorithm's ability to accurately match a photo from a sample gallery of millions of images, its algorithm ranked first in the US, second in the world and was in the top 10 in all categories out of 328 algorithms tested[111].

Still on certifications and tests, in February 2022, Clearview A.I. achieved the highest standard in cybersecurity certification[112]. The System and Organization Controls 2 - SOC 2[113] test certified that the company maintains adequate controls over its users' data processing security and integrity. According to Hoan Ton-That, the SOC 2 test undertaken by BARR Advisory, P.A. “demonstrates that we have the appropriate controls in place to ensure the security and accurate processing of the data entrusted to us by law enforcement clients". The company's "NIST FRVT Results for Clearview AI"[114] document emphasizes that the algorithm is 99% accurate across all demographics in the more complex "wild photos" category. On one hand, "in the wild" is an ideal feature for training and testing data of facial recognition algorithms because it can provide a closer match to an unknown deployment environment, which would improve real-world performance by

[109] Available on: https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf. It was accessed on November 02, 2023.
[110] Ibid.
[111] Ibid.
[112] Clearview AI Maintains Effective Security Controls SOC 2 Report Certifies. Available at: https://www.clearview.ai/press-room/clearview-ai-maintains-effective-security-controls-soc-2-report-certifies. Accessed on: Nov. 10, 2023.
[113] SOC 2 is an auditing procedure conducted by certified, licensed, and regulated public accountants, which rigorously analyzes data service providers to ensure the secure management and accurate data processing.
[114] Available on: https://app.hubspot.com/documents/6595819/view/449537243?accessId=b92ab6. It was accessed on November 02, 2023.

reducing biases and prejudices (ZAFEIRIOU et al., 2015). On the other hand, data collected from sources "in the wild" inherit new problems, including systemic inequalities in society, and are never "wild" (KAUFMANN, 2020). Therefore, representing datasets as unrestricted or "wild" simplifies the complexities of the contexts in which these technologies are applied and reinforces ways of seeing and understanding these contexts.

While these tests authorize Clearview to be claimed as a "validated, dependable, and fair" algorithm, a careful reading of the NIST report allows us to explore the limits of its demographics. Clearview's algorithm was better at identifying men than women - in all categories - and was more likely to confuse the faces of people born in Nigeria and Kenya than those born in Poland. As we analyzed in the previous chapters, algorithmic discrimination results from a lack of diversity in the training data that produces biases – a matter which is not easily solved with technical corrections and technology optimization – as claimed by Clearview. As Benjamin (2019, p.160) argues, the effects of algorithms must be analyzed through broader socio-political processes, meaning that any purely technical-scientific approach aimed at overcoming its limits is a simplification of complex issues. Furthermore, those approaches end up reaffirming that Clearview may be a "bias-free" algorithm that would bring more justice and efficiency to security practices.

Clearview AI presents itself as unprejudiced and technologically superior to other technologies in terms of accuracy and the possibility of accountability by having protocols that entangle the decision agent in the security loop. As we will see in the following sections, these frameworks legitimize the materialization of the algorithm in different spaces of its current use and authorize the expansion of its use towards other domains.

4.3. “Controversial facial recognition”

As we noted in section 4.1, after the company "came out of the shadows" in early 2020 (HILL, 2023), Clearview AI's security solutions took center stage in the debate about the expansion of the use of facial recognition technologies and the challenges concerning fundamental human rights. If such centrality posed challenges to the company's development, it also generated curiosity and gave

impulse to the promotion of the company to potential users unaware of its existence. At this point, Clearview AI's website has a "Media Highlights" tab that includes links to various controversial subjects and articles that mention the company.

Controversies imply the contestation of values and identities, but even more so the definition of the problem as such (CALLON; LASCOUMES; BARTHE, 2009, p.25) and help to understand how specific truth claims came to be recognized as "facts" (LATOUR, 2003). To map the controversies involving Clearview AI, I analyzed online media data from January 2020 to July 2023 collected from the Media Cloud[115] platform, documents published by Clearview AI, publicly available interviews and the content of the company's presentations at Copaq/SENASP, LAAD Defense & Security 2023 and ISC Brasil 2022. This section aims to map the controversies and criticisms of using the software and reflect on how these discursive and material practices are fundamental to understanding how the algorithm has come to be crystallized as a sufficiently efficient security solution.

Figure 16. Media Analysis on Clearview AI over time

Source: Prepared by the author with data collected from Media Cloud.

[115] Used for quantitatively studying online media, Media Cloud is a big data platform emerging from the collaboration between Civic Media and the Berkman Klein Center for Internet and Society at Harvard Law School. The platform is open source and open data, designed to be a substrate for a wide range of communication research efforts. The Media Cloud search used the keyword "Clearview AI" across all English-language media in the following sets: US mainstream media, US regional media, US political blogs, US popular blogs, Europe Media Monitor, and Global Voices. The date range from January 1, 2020, to July 11, 2023. Available at: https://www.media.mit.edu/projects/media-cloud/overview/ .

According to the media data analyzed, the graph visually represents the frequency with which Clearview AI has been mentioned in the media over time. Clearview points out that it has become more involved with the media "to build understanding and trust with the public (…) to inform them about what our technology does"[116]. As shown in Figure 10, the amount of attention paid to the software had a significant increase in 2020 and over time has zigzagged until another peak, not as intense as the first, but higher than the others referring to news of the use of software in the war in Ukraine[117]. In particular, 52.44% of the total news stories about the company in the database created by the Media Lab are from 2020. Of these news stories, I observed ten keywords that most recurrently appear in the headlines: "Clearview AI," "face recognition," "privacy," "controversial," "police," "surveillance," "data," "ban," "stop," "Facebook." Together with the analysis of documents and interviews, I was able to draw a map of controversies whose nodal points are: privacy, data collection without consent and surveillance; accuracy and bias; and opacity. These nodes reflect the broader debate on machine learning algorithms used in security practices, as analyzed in section 2.3.

Privacy and mass surveillance

From a general perspective, the Clearview case fits into a global trend of reusing data collected by the private sector for law enforcement purposes (FERGUNSON, 2017; RUPPERT et al., 2019; CRAWFORD, 2021; HOFFMANN, 2018). Many transparency reports show that law enforcement agencies increasingly request access to data stored by tech giants such as Facebook, Google, and Microsoft (ANSWAR, 2021; REZENDE, 2021). Government agencies have sometimes begun purchasing personal data from private companies to circumvent legal safeguards around law enforcement access to database commerce (i.e. subpoenas or court warrants) (BAYNE, 2017). However, the use of Clearview differs from other scenarios involving the disclosure of personal data from the private sector to law enforcement. Personal data is not transferred to law enforcement on a case-by-case basis, for a fee or under a legal obligation: it is

[116] AI Insight Forum - Statement by Hoan Ton-That, CEO of Clearview AI - November 1, 2023. Available at: <https://www.clearview.ai/ai-insight-forum>. Accessed on: Nov. 7, 2023.
[117] On this topic we will discuss in section 4.4.

collected by a private company to make it available, through an institutional arrangement, to government agencies for law enforcement purposes.

The ambivalence about the accuracy and reliability of Clearview AI's facial recognition algorithm goes hand in hand with the problematization of the directory and database on which the algorithm depends. The US company's data collection method has generated criticism from human rights defenders, academics, and government data protection organizations (REZENDE, 2021; MCSORLEY, 2021). As previously noted, the company's database plays a key role in marketing campaigns while also attracting law enforcement agencies. However, this access to data has been the subject of much public criticism because it compromises the privacy rights of both individuals and the platforms from which the images are taken. The transparency of digital platforms' terms of use and privacy policies involving personal and sensitive information is being questioned in public debates regarding Clearview AI. Also, it raises the alarm of the possible expansion of surveillance to scalar levels, especially of subjects and groups usually perceived as a threat to order. One problematic example is the use of the tool to identify subjects perceived as "radicals" in protests, as we saw in chapter 3.

It is in this context that calls for data security and privacy guarantees take place. Some speeches support the policies of sharing personal information for security purposes, nevertheless. One of the most recent "success stories" reported by Clearview AI of the use of the algorithm to solve complex crimes occurred in October 2021, when the technology was used to identify a perpetrator in a significant case of child sexual abuse in Las Vegas that led to a 35-year prison sentence[118]. The "success stories" in apprehending criminals and solving crimes have been connected to the discourse that the Clearview AI algorithm is efficient and a necessary resource for security agencies. Clearview claims it "exists to help law enforcement agencies solve the most difficult cases."[119]

According to a 2019 internal document, Clearview AI had plans to carry out a "rapid international expansion" in at least 22 countries (HASKINS; MAC;

[118] Available at: https://www.clearview.ai/post/fed-agency-identifies-suspect-of-las-vegas-child-exploitation-in-background-of-social-media-profile Accessed June 15, 2023.
[119] Available at: https://www.eff.org/pt-br/deeplinks/2020/01/clearview-ai-yet-another-example-why-we-need-ban-law-enforcement-use-face Accessed June 15, 2023.

MCDONALD, 2020). In February 2020, the company's strategy focused its investments on the US and Canadian markets, but with the continued insistence on offering free tests to security agents from various European countries by actively participating in police conferences, such as Europol's European Cybercrime Center in 2019 in the Netherlands (MAC; HASKINS; PEQUENO, 2021). The company recorded an increase in peak usage and test requests in the United States after its software came to be considered as an "essential" tool for recognizing the Capitol attackers on January 6, 2021 (HILL, 2021). Its use as a tool for identifying intruders and other kinds of threats is mobilized as part of its “success” in folders and other marketing materials of the company – a discourse that found increasing adherence among military, law enforcement, and migratory agencies (GAO, 2021).

The event on Capitol Hill was important in stressing the importance of technology in solving national security issues (see Figure 11). We can see from the news analysis that there has been a significant and notable change in perceptions about facial recognition technology at that period. According to Hill (2023), before that particular event, public opinion was more concerned about the use of facial recognition; afterwards, the identification of invaders with the support of those facial recognition technologies came to be seen as necessary.

Figure 17. Folder distributed by Clearview AI

Source: digital scan of the folder handed out at LAAD on April 14, 2023.

We can observe the presence of dichotomies between privacy and security that are invariably reproduced in conventional public debates about surveillance technologies (BAUMAN et al., 2015). However, it is essential to reflect on the limits of these dichotomies when we analyze the complexity of the formation of the data repository (public data posted on the Internet voluntarily by users), the processing of the Clearview algorithm, and its use by security agencies. In 2020, the ACLU sued Clearview for violating the Illinois Biometric Information Privacy Act (BIPA), state law that prohibits the capture of individuals' biometric identifiers, such as face and fingerprints, without prior notice and consent (ACLU, n.d.). As a result of this lawsuit, Clearview AI was prevented from selling the tool to private companies[120]. While some privacy experts have described this agreement between the ACLU and Clearview AI as a "watershed" in advancing data protection and privacy (DEGEURIN, 2022), the agreement did not change the company's business objective. Indeed, the company continued to expand the circulation of its facial recognition technologies among government security agencies, its most poignant market, in compliance with applicable legislation.

The ACLU also represented a group of organizations whose members and service recipients are particularly vulnerable to non-consensual facial impressions and surveillance: survivors of domestic violence and sexual assault, undocumented immigrants, current and former sex workers, and individuals who regularly exercise their constitutional rights to protest and access reproductive health services. Clearview's defense argued that to create its facial recognition algorithm, it gathered publicly available photos from all over the Internet and then used them to run a search engine that expressed Clearview's opinion (language by the code) of who appeared to be in the photos. Thus, the company claims that, as a search engine, it has a First Amendment right to disclose information already available online[121]. The use of the First Amendment by a tech company to anchor the legality of its practices is not new: Google has used this argument to deal with attempts to regulate its search engine. In 2020, TikTok sued the U.S. based on former President Donald

[120] Available at: https://www.clearview.ai/clearview-ai-settles-aclu-illinois-lawsuit-confirming-continuity-of-business-supporting-publics. Accessed June 15, 2023.
[121] Available on: https://slate.com/technology/2020/11/clearview-ai-first-amendment-illinois-lawsuit.html . Accessed June 15, 2023.

Trump's executive order to shut down the platform's activities in the country[122]. The argument stated that the order violated the First Amendment because TikTok runs on code, and code is words – a type of language[123]. The regulatory agencies of several European countries have banned the use of the tool under the assessment of the European General Data Protection Act (GDPR), which establishes that the processing of sensitive personal data requires the explicit consent of individuals (REZENDE, 2020). Australia and the UK also have accused Clearview of violating their privacy and data protection laws. Canada's Office of the Privacy Commissioner is investigating the company's activities in Canada (MCSORLEY, 2021).

Thus, Clearview AI is facing increasing scrutiny based on data protection rules, even in the US, which does not have a federal data protection law. In response to the public and regulatory debate around the use of the tool and in order to comply with data protection legislation, Clearview AI currently has a data protection policy displayed on its website that can change depending on the respective jurisdiction. For example, the California Consumer Privacy Act allows residents to request a copy of the data companies like Clearview hold about them, and there are now similar provisions in the European Union. Some laws stipulate that data stored in the Clearview AI database can be deleted at the user's request.

Regarding criticisms about the relaxation of privacy and the possibility of mass surveillance, in the document titled "Response to Open Consultation UK Surveillance Camera Commissioner" (2021)[124], Clearview AI reinforces that it does not have any products or any technology that performs real-time facial recognition, but that the tool is a face search tool to be used in investigations by security agencies "respecting fundamental rights, freedoms, and democratic values." Moreover, the company claims that it has developed a series of good practices in facial recognition, that the software's use is limited to "socially beneficial" purposes, and that it complies with the principles established in the Code of Practice. When asked about the controversies surrounding privacy and the possibility of misuse of the

[122] Ibid.
[123] Available on: https://www.euronews.com/next/2022/05/10/facial-recognition-company-clearview-ai-permanently-banned-from-selling-data-to-private-co. Accessed June 15, 2023.
[124] CLEARVIEW AI. Response to Open Consultation UK Surveillance Camera Commissioner. 8 set. 2021.

algorithm, the company's CEO insisted on the tool's efficiency in solving security issues:

> We could show a lot of examples of a lot of success stories from Indiana state police, FBI, Homeland Security, etc. So, it's totally worth engaging with the media and since then there's been a lot of controversy but fundamentally this is something that's such a great tool for society[125].

In the documents and interviews examined, Clearview AI argues that its practices do not constitute mass surveillance, for its technology only operates with the intervention of a security professional. As noted in the previous section, however, an API that allows integration with other software suggests the feasibility of adapting this technology for use in real-time. This possibility is even more evident with the recent launch of the company's augmented reality glasses called the "Vuzix blade"[126], which was granted by the US Air Force a US$50,000 investment aimed at stimulating research and testing (HARWELL, 2022).

Many in academia have also reacted to the "revolutionary facial recognition algorithm. The University of Chicago lab presented a "solution" for scraping Clearview data from our photos posted online. A tool called Fawkes was developed to subtly alter the parts of an image that facial recognition uses to distinguish one person from another while trying to preserve the image's appearance for humans (SHAN et al., 2020). Nevertheless, this would depend on the individual rendering all their newly posted photos and not implying the ones already in the company's database.

Professor Ben Zhoa, supervisor of the project, points out that "avoiding Clearview will require more than just a technical fix or a little push on Facebook's privacy check" (VICENT, 2021). Indeed, the privacy issue is not just a technical matter, nor one that can be easily solved by regulations and laws, or limited to

[125] The podcast interview "This Week in Startups" is hosted by Jason Calacanis, a technology entrepreneur, and covers startups, technology, markets, media, and the hottest topics in business and technology. The program reviews the latest news related to new tech startups, often featuring the founders of various internet companies as guests. Available at https://www.youtube.com/watch?v=wNLK_f6m4e0&t=44s (18:45).
[126] Copaq/ SENASP presentation - February 09, 2022.

Clearview AI. It is also a matter of how the algorithmic reason has been stabilized and operated with the amount of data.

Accuracy and Bias

Can the biases in facial recognition be fixed? Should they be fixed? This question is another nodal point in the criticism of the implementation of their use in security practices and their possible banning, especially in policing. Here, the concerns related to security agents using Clearview refer to the possibility of errors, low accuracy, and bias that would perpetuate stigmas and legitimize exclusionary and violent practices. Seminal studies such as Boulawnini and Gebru (2018) have shown how facial recognition technologies vary in their level of accuracy in different demographic groups, which would reinforce social discrimination, especially concerning non-white people. As analyzed in the previous chapters, the issue of bias and error has been part of the debate on the use of facial recognition algorithms since they emerged as a possibility to automate previous biometric identification practices.

Facing this increasing debate since 2020, Clearview AI has discursively framed its algorithm as efficient and objective. However, no tests among those carried out offer cement to the technical legitimation of this discourse. As we have seen, there was already a growing body of academic research and reports from non-profit organizations pointing to bias and a significant gap in accuracy. The test carried out by the ACLU in 2019 with Amazon's Rekognition tool, which at the time was the most widely used by US security agencies, demonstrated how much the tool misses; it misidentified 28 congress members photos in the trial. The findings influenced political discussions and social debate, culminating in several public security agencies' campaigns to ban these technologies.

The incidence of social organizations and the ACLU test in this debate can be illustrated by the fact that Amazon, Recognition’s supplier, implemented a one-year moratorium on the sale of technology to the police (MAGID, 2020). In addition to that, there has been an increase in social and political demand for the developers of these technologies to improve accuracy in order to minimize errors and bring "justice and ethics" to these systems, as well as a change of course in the sector

itself (PESSACH; SHMUELI, 2023). Furthermore, in June 2020, the Association for Computing Machinery called for a halt to private and government use of facial recognition technology on the grounds of a "clear bias based on ethnicity, race, gender, and other human characteristics," claiming that it violated the rights of people in specific demographic groups.

In this context, companies supplying facial recognition technologies themselves have sought to assist in establishing specific levels of acceptability and regulatory standards. A concrete example was the request filed by three of the largest suppliers of algorithmic technologies to law enforcement agencies (Amazon, IBM, and Microsoft), asking the US Congress for legislative measures on facial recognition systems, offering all the help necessary to create possible regulations for the sector. In the specific case of Clearview, the company subjected its algorithm to the same methodology as the ACLU's test with images of members of Congress in an independent panel that classified the algorithm as 100% accurate in all demographic groups[127].

When a company lists only one accuracy metric, this is necessarily an incomplete view of the accuracy of its system because, depending on what the system is designed to do, this may have little or no influence on the actual accuracy of the system in practice. However, these tests perform an important role in quantifying accuracy, thereby validating systems. Indeed, although it lacked rigor, Clearview's test worked to show that its facial recognition technology was superior to Amazon's Recognition in a context where the company was focused on expanding use by government agencies (HILL, 2023, p.205).

Another reaction of the company as regards criticism on bias was the publication by Ton-That of a text blog in 2022 titled "The Myth of Face Recognition Bias"[128], in which he presents the "methodological flaws" of both the research undertaken by Boulawnini and Gebru (2018) and the one by ACLU (2019). According to him, circulating since 2018, the "myth" was that facial recognition

[127] CLEARVIEW AI. ACLU's test results of Amazon's Rekognition AI Facial Recognition Technology Debunked. Available on: https://www.clearview.ai/post/aclus-test-results-of-amazon-s-rekognition-ai-facial-recognition-technology-debunked. Accessed June 15, 2023.
[128] CLEARVIEW AI. The Myth of Facial Recognition Bias. Available at: https://www.clearview.ai/post/the-myth-of-facial-recognition-bias. Accessed June 15, 2023.

technology is notoriously inaccurate and racially and demographically biased, leading to criticism from activists. To confront that “myth”, he mobilizes data from NIST tests showing that this technology has gone through significant advances, increasing its accuracy and surpassing, in some respects, "the ability of the human eye to recognize faces." According to Ton-That, the most updated versions of the algorithm reveal high technical-scientific development, and "proven" accuracy in its use to solve the problems of wrongful arrests. In his words:

> It is important to know the facts and science when discussing life changing topics like the use of FRT in law enforcement, potential legislation, or regulation. Clearview AI believes that regulation is essential for powerful technology like FRT, and all the facts about the accuracy of the technology must be known before making any judgements or decisions regarding its use. (...) In the last 3 years of Clearview AI being deployed in the field, there have been no known wrongful arrests due to the use of our technology.[129]

Here, we witness the discourse of an objective and unbiased facial recognition tools, different from previous versions of technologies of the kind, making a reliable resource for the identification of errors, and not their cause – as suggested by the critics. As already noted, the "solution" to "algorithm problems" has repeatedly been framed in terms of technical corrections (e.g. database diversity) and technology optimization.

According to Gebru (2019), framing anti-bias measures as equalizing performance between groups does not answer questions about whether a task should exist in the first place, who creates it, who will deploy it in which population, who owns the data, and how it is used. As argued in the first pages of this dissertation, the algorithm does not operate in isolation; it is a socio-technical system in which many practices are entangled. For this reason, focusing on technical development decisions oversimplifies the issue of biases and their effects and relegates the possibility of a "solution" to a specific field of experts.

An additional contentious point regarding the accuracy of Clearview facial recognition technologies refers to situations in which computer vision algorithms have more influence than people's direct testimony or when a community cannot

[129] Ibid.

challenge the algorithmic decision due to a lack of ability to express their knowledge in equivalent ways (SYMONS; ALVARADO, 2022). When algorithms provide information and answers about someone's identity, the testimony and active participation of individuals or groups without access to this information is devalued, even when they are the main targets. There are diverse and dispersed power relations that sustain algorithmic workflows and create the conditions of possibility for framing it as reliable and "perfectible" while at the same time underlining its contingency. As a result, the authority with which algorithms came to enjoy can perpetuate inequalities and exclusions through errors or false positives and amplify epistemic injustice (AMOORE, 2020).

We can observe in this dissertation that the errors and challenges have produced ambivalence in the material-discursive practices of using facial Recognition in security practices, generating pauses, and reshaping what is considered a reliable standard of operation. In these spaces, in the cracks of criticism, many intra-actively material-discursive practices have created conditions for the materialization of facial recognition algorithms such as Clearview. After all, failure is a feature of machine learning algorithms, not a bug. This characteristic implies that not only can there be an optimal solution but that other possibilities are sub-optimal by definition (MACQUILLAM, 2022) in a constant search for a "pattern" that works. Critical work on the training data used to test the quality of algorithm standards shows that these are reuses of contested data while supporting neutral standards (KEYS et al., 2019; THYLSTRUP; HANSEN; AMOORE, 2022). As Stengers (2000, p.17) points out, we need to be aware that specific modes of critique can paradoxically affirm the power they seek to denounce.

Opacity

Opacity is also one of the central nodes of criticism of Clearview AI. Media reports recurrently present Clearview AI as a "black box," an "opaque," and "obscure company". Importantly, the "black box" discourse is part of the framework in which algorithmic reason has crystallized and circulated in different contexts and uses, as we analyzed in chapter 2. Due to the difficulty of attributing responsibility to what causes suspicion of being guided by obscure computational forces, 'algorithm' has emerged as the perfect and captivating word, symbolizing an

increasing opacity and dehumanization in the practices entangled with it. Blaming "algorithm" for the opacity inherent in computer technologies is a current attempt to circumscribe the problem to an identified, even if unknowable, cause. In Clearview's case, this is due both to the lack of transparency in the operations of its algorithm and its data collection and also its business model, which, with free trials, does not produce records, making it difficult for the public to scrutinize which agencies are using the technology[130].

Moreover, there is almost no oversight even when the use is publicized, according to a new report released by the United States Government Accountability Office (GAO, 2023). According to the report, 20 different agencies - from ICE and the FBI to the Department of Veterans Affairs - were found to be using facial recognition. Among those, 17 of the agencies relied at least partially on Clearview AI technology[131]. The report's data indicates that 6 out of 7 federal agencies prefer Clearview AI to other private facial recognition technologies. Nevertheless, almost none of the agencies knew which systems employees were using; in other words, administrative oversight of usage was low. Another noteworthy aspect of the report is that 95% of FBI agents who used the technology did not complete training on the protocols for using the technology offered by the company. The FBI has no policy on using facial recognition technology to safeguard against misuse, which could make fundamental rights more flexible.

The problematization, discursive circulation, and political responses to technological problems have been shaped by ambiguous figures such as the "black box" or the "biased algorithm." In a context where the materiality and agency of algorithms are heterogeneous, figures that fix complex and multiple assemblages into a single entity simplify the debate and reinforce a public perception of the (im)possibility of understanding algorithmic practices. However, before being black box engines of computational orders, they were everyday practices of

[130] This has been observed in Brazil, as described in the following Intercept Brasil article: MARTINS, L. Exclusivo: Clearview ofereceu fotos de brasileiros para polícias e Ministério da Justiça. Available at: https://www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/>. Accessed on: 11 Nov. 2023.
[131] FACIAL RECOGNITION TECHNOLOGY Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks Report to Congressional Requesters United States Government Accountability Office. [s.l: s.n.]. https://www.gao.gov/assets/gao-21-518.pdf Accessed on: 11 Nov. 2023.

different human and non-human actors circulating in various areas of society. Ultimately, what must be negotiated and governed is not just a digital object but a set of protocols and procedures comprising organizational habits, legal rules, analog artifacts, and technological knowledge

4.4 Debugging: re-use, optimization and expansion

'Debugging' is a common term in computer science to refer to identifying, isolating, and correcting flaws or bugs in a software. Such process is a fundamental part of software development and it is crucial for guaranteeing an algorithm's quality, functionality, and efficiency. This algorithm debugging process is intra-active, where the programmer, algorithm, development context, and bug are entangled to generate an optimized output. I open the final section of the chapter with this computational metaphor to trace the thread I have followed so far and outline that the flaws, the moments of pause, the critical frictions, and the reorientations of use are not 'bugs.'

The role played by algorithmic reason in security contexts is to convey more efficiency or innovation to actions - the performative figure has normative effects of naturalizing the search for endless optimization. Here, the staging of algorithms strengthens the discourse of technological determinism (CRAWFORD,2013; 2021). It could explain how, amid controversy and sanctions, Clearview AI received a round of funding in July 2021 of US$30 million and became worth US$130 million. According to the company's website, this investment includes funds from institutional investors and family offices that "will fuel Clearview AI's continued growth."[132] It has also expanded its hiring and created a strategic advisory board, mainly made up of people from the law enforcement and US government sectors, such as former New York City police commissioner Raymond Kelly and former National Security Council senior official Richard Clarke, who served during the Bush and Clinton presidencies. Clearview AI has been reshaping and debugging its algorithm and practice to expand its market, even amid litigation and criticism.

[132] Clearview AI Closes 30 million Dollar Series B Funding Round. Available at : https://www.clearview.ai/press-room/clearview-ai-closes-30-million-dollar-series-b-funding-round#:~:text=NEW%20YORK%2C%20JULY%2026%2C%202021,the%20company%20at%20%24130%20million .Accessed on: 11 Nov. 2023.

In the United States, its primary market, in 2021, the GAO released its initial review of the use of facial recognition technology in federal security agencies. The report found that at least half of the 24 agencies examined were using Clearview's facial recognition technology, showing that 10 of the 24 agencies surveyed plan to expand their use by 2023[133]. Some federal agencies that are known to use facial recognition are outside the scope of this specific report, and no comprehensive research on government use of the technology has been done to date. A follow-up to this GAO assessment released in July 2023 shows the widespread use of the technology in US security agencies at the local, state, and federal levels. These figures still need to be revised; as we have seen, tests allow for use without formalized organizational knowledge. Finally, the US Department of Defense's Air Force and the Department of the Interior's Fish and Wildlife Service have been working on projects with Clearview AI that the agencies plan to expand[134].

As we saw in the previous section, with the controversies surrounding the company, especially in 2020, it can be seen that as the company gained notoriety in the United States, the Canadian and European markets began to restrain to the use of Clearview AI by their security forces, culminating in bans which are still active in several countries. However, despite the "closing of some doors," the company has been preparing the ground for expansion, not only geographically but also in the form and purpose of the uses of its technology: "humanitarian uses" and the "JusticeClearview" offered to public defenders (CLEARVIEW, n.d.).

In 2022, Clearview "goes to war," in the words of The New York Times[135]. After the Russian invasion of Ukraine, the company saw another potential use for its technology: improving security and humanitarian efforts. In an interview, the company's CEO said: "We saw images of prisoners of war, of people fleeing, and we thought that our technology could be useful for identifying people and

[133] FACIAL RECOGNITION TECHNOLOGY Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks Report to Congressional Requesters United States Government Accountability Office. [s.l: s.n.]. https://www.gao.gov/assets/gao-21-518.pdf Accessed on: 11 Nov. 2023

[134] Ibid.

[135] Facial Recognition Goes to War. Available at: https://www.nytimes.com/2022/04/07/technology/facial-recognition-ukraine-clearview.html Accessed on: 11 Nov. 2023.

verification."[136] In a letter sent to the Ukrainian government, Ton-That claimed that Clearview's technology could "help Ukraine defend itself against Russian invasion," which included reuniting refugees separated from their families, identifying Russian agents, and helping the government debunk false social media posts related to the war[137]. The company made the tool free of charge to the Ukrainian government, and the use "spread quickly." Currently, seven Ukrainian agencies use it (data until December 2022)[138].

The company invites visitors to read "How Clearview AI Helped Shape the War in Ukraine" on its website. According to the company, "each search had the potential to save a life at a checkpoint, help ID missing person, and more."[139] Clearview has been used for the following functions in Ukraine:

1. Identifying the dead quickly and tracing families to inform them of the death.
2. Identifying people in refugee camps who have no documentation or identification.
3. Intercepting potential infiltrators who may be "posing as Ukrainians."
4. Building "a relationship with captors to facilitate effective interrogation by understanding their background."[140]

In April 2023, CEO Ton-That received an award for "Important contribution and dedication of time and efforts to provide volunteer services to the Ministry of Defense of Ukraine" from General Kyralo Budanov, Head of the Main Intelligence Directorate of the Ministry of Defense of Ukraine[141].

[136] Como reconhecimento facial é usado para identificar mortos na Ucrânia - BBC News Brasil. Available at: https://www.bbc.com/portuguese/internacional-61104864. Accessed on: 11 Nov. 2023.
[137] War in Ukraine - Clearview AI. Available at: https://www.clearview.ai/ukraine. Accessed on: 11 Nov. 2023.
[138] Ibid.
[139] Ibid.
[140] Copaq/ SENASP presentation - April 13, 2022.
[141] Hoan Ton That CEO of Clearview AI presented with an award by General Kyrylo Budanov of the Main Directorate of Intelligence of the Ministry of Defense of Ukraine. Available at: https://www.clearview.ai/press-room/hoan-ton-that-ceo-of-clearview-ai-presented-with-an-award-by-general-kyrylo-budanov-of-the-main-directorate-of-intelligence-of-the-ministry-of-defense-of-ukraine Accessed on: 11 Nov. 2023.

We note that the materialization of Clearview AI in the Ukrainian context brings different contours and possibilities of practice and other ethical, political, and social concerns about its use. It is important to note that testing algorithmic technologies, especially biometric ones, in humanitarian contexts has been normalized. Refugee camps worldwide have been laboratories for testing various surveillance technologies (see more in PARKER, 2019). As noted in chapter 3, the colonial legacy of datifying bodies that need to be watched and controlled remains. Scott Smith (2016, p. 2230) coined the term "humanitarian neophilia" to define a technosolutionist ideology that 'combines an optimistic faith in the possibilities of technology with a commitment to the expansion of markets.' The uses of the Clearview AI algorithm are being tested, adapted, and expanded. In the presentation made in Brazil, the company's representative states that the technology is proven in a war context. In other words, it has been tested and evaluated as successful[142].

The other "positive" use of Clearview AI was its interface for public defenders, "ClearviewJustice." The application of the algorithm was sparked by a request from Christopher O'Brien, a public defender, who asked if he could use the tool to prepare a defense. The defender used the algorithm to identify another witness in the case from the police body camera video, and after the witness testified, the vehicular homicide charges were dropped[143]. As this case reveals, reuse and reconfiguration are part of algorithmic reasoning. In September 2022, Clearview launched its interface for public defenders, the first facial recognition product aimed at defenders to "do justice"[144].

> Clearview AI's mission to seek justice and support public safety goes beyond helping to identify those who commit crimes; it also includes helping to exonerate those who have been wrongly accused. These are two sides of the same coin and are equally crucial for the proper administration of justice for victims of crime and the general public[145].

[142] Copaq/ SENASP presentation - April 13, 2022.
[143] Available at: https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html#:~:text=Google's%20Bard%20Extensions- Accessed on: 11 Nov. 2023.
[144] Clearview AI Launches JusticeClearview First Facial Recognition Product for Public Defenders Seeking Justice. Available at: https://www.clearview.ai/press-room/clearview-ai-launches-justiceclearview-first-facial-recognition-product-for-public-defenders-seeking-justice . Accessed on: 11 Nov. 2023
[145] Ibid.

Clearview classifies the technology as efficient, affordable, and justice served. The purpose is to allow for public defenders to being able to do more with fewer resources. The evidence generated by the algorithm supported by other evidence would help to "accurately and quickly identify other witnesses or persons of interest who could change the course of justice"[146]. The ClearviewJustice tab on the company's website presents data showing that Clearview is the fastest and most accurate solution to wrongful convictions. According to the company, 80% of criminal cases involve video evidence, and 70% of wrongful convictions that were overturned by DNA evidence stemmed from eyewiness identification. These figures are the basis for the company to claim that it is "Scientifically proven that facial recognition technology is more accurate and less biased than the human eye" (CLEARVIEW, n.d). In other words, the tool can analyze vast image data more reliably than a human, generating more accurate and neutral evidence.

We can see from the analysis of Clearview AI how its discourse and use have been adapted and adjusted or not to the criticisms and debates in which it has been inserted. As Parisi argues (2013, p.2), the final target of machine learning algorithms can be anything. A policy operates through these adjustments and cooperates to build technical credibility – through the acquisition of patents – and use, always pointing out how the security and even "humanitarian" benefits outweigh the relaxation of rights such as privacy. If "the doors to Clearview are closing in the markets of the Global North," as the article in the MIT Technology Review (2023) points out, growing markets for policing technologies, such as in countries of the "Global South" like Brazil, look attractive, as well as the expansion to other uses.

Finally, I note that the Clearview AI algorithm is a figure or summary to describe a complex set of interactions, a way of synthesizing a set of entities that shape and reorder a "borderless" algorithmic context (ANANNY; CRAWFORD, 2016, p.11). Clearview operates in a "game of indeterminacy" (BARAD, 2007) and reconfiguration, composed of a multitude of dispersed and, at the same time, entangled practices. Rather than depoliticizing or neutralizing these materializations of the Clearview algorithm, it is important to note how deeply

[146] The use of Clearview as "support" evidence will be explored further in the next Chapter.

political they are, with ambivalent material-discursive implications gaining traction. Regardless of the data they have been trained on, algorithms are always partial and experimental, generating new boundaries between normal and abnormal, good and bad, and new ways of seeing and doing. It means, as argued by Jasanoff (2016, p.34), that "the idea of zero risk – that is, of a perfectly functioning technological environment in which machines and devices do exactly what they are supposed to do and nobody gets hurt – remains an unattainable dream." Perhaps we should then reflect on what conditions of possibility underpin Clearview AI's discourse according to which it is possible to "Build a secure world one face at a time."

5.
What algorithmic evidence makes possible: face recognition errors and failures in practice

On August 7, 2020, "Warriors in The Garden"[147] activist, part of the "Black Lives Matter" movement, Derrick Ingram, 28, was surprised at his home by a group of New York City police officers, including some with riot gear, drones, and helicopters. Derrick was accused of assaulting a police officer during the June protests[148]. The officers did not have a search and seizure warrant (a legal requirement). However, a document titled "Facial Identification Section Informational Lead Report" includes evidence produced by Clearview AI's facial recognition algorithm: a photo posted on Derrick's Instagram.

The activist did not open the door to ask the officers for the warrant. Officers tried to break down his door and interrogate him without a lawyer and set up for hours in his hallway, on his fire escape, and in tactical positions in and around nearby buildings. The police left the building only after Derrick had live-streamed the events on his Instagram account, demonstrators gathered for a protest, and the press started covering the case[149].

This is not a unique case. The Miami police, using body camera footage from the officers and the same Clearview AI software, identified and arrested Oriana Albarnoz, 25, also a Black Lives Matter activist. Unlike Derrick, they had a warrant, and the charge against her was throwing rocks at a police officer. Oriana's lawyer, Mike Gottlieb, had no information on how she had been identified. The police did not mention the use of facial recognition technology in the arrest report, only stating that she had been "identified through investigative means." It is important to note that protests are protected activities under the US Constitution. In this sense, the use of facial recognition algorithms to identify and punish protesters

[147] "It is a collective of activists dedicated to non-violent protest who are committed to protecting the Black community from police brutality and all forms of systemic oppression.". Warriors in the Garden. https://warriorsinthegarden.org. Accessed December 13, 2020.
[148] CNN. Available at: https://edition.cnn.com/2020/08/09/us/new-york-black-lives-matter-activis. Accessed on: December 9, 2020.
[149] AMNESTY INTERNATIONAL USA. Available at: https://act.amnestyusa.org/page/66572/action/1?locale=en-US . Accessed on: December 9, 2020.

is anchored in a discourse that these are only used on "radical" subjects or "violent protesters."[150]

Despite being an open concept, due process is fundamental to guaranteeing rights in legal systems. This basic constitutional principle gives individuals the right to understand what they are accused of and the evidence against them. In the cases reported, using facial recognition software from Clearview AI created the conditions for recognizing a protester perceived as enough "radical" to be arrested. These two cases reveal how procedural safeguards are relaxed to ‘mitigate security risks’ based on evidence from facial recognition algorithms using biometric data.

As noted in the Part 1 of this dissertation, machine learning algorithms are inventive: they suggest what "might be"; they operate a "surface rationality" (KRASMAN, 2019) in which what is important is what is visible, the behavior that can be traced by the security professional, the individual that can be recognized. What can be seen or identified as a pattern provides the algorithm/ who evidence for the meaning of a particular behavior and action. The very idea of the "emerging subject," the subject that becomes visible and recognizable through algorithmic techniques (AMOORE, 2013), is central to the ongoing efforts of security policies to deal with the "radicalization problem," which spills over into everything that deviates from the midpoint social conduct as discourses on criminals and terrorists.

As I have pointed out in this research, facial recognition by security agents in the United States and many countries worldwide has become a norm. Although the number of arrests, charges, court decisions, based on the use of such resource is unknown (GARVIE, 2022), facial recognition algorithms, including Clearview AI, have been increasingly mobilized framed as stepping stones to an investigation. In the absence of guidance, in some cases, it has been claimed as the only evidence providing the causal link between an individual and a crime. However, the subjects 'recognized' by this evidence and charged on its grounds are often deprived of the opportunity to challenge it.

[150] THE VERGE. Available at: https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram . Accessed on: December 9, 2020. THE WASHINGTON POST. Available at: https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban/ . Accessed on: December 9, 2020.

Despite growing use, the reliability in criminal investigations and its use as criminal evidence has yet to be established. Indeed, defense lawyers, prosecutors, judges, and security agencies are unclear about how the algorithms are used. As we have seen in the previous chapters, there is minimal transparency about how these algorithms are used in practice and how the evidence they produce has been framed. The use of Clearview AI through free trials without a police department acquiring a license is just one of the examples of how the diffusion of facial recognition algorithms has happened flexibly, a practice that can be (re)modeled in each organizational context. At the same time, the damage and violence of stop-and-frisks, detentions, and erroneous investigations anchored in the probabilistic results of the algorithm materialize actions, although it is difficult to quantify them. Most security agencies that use the technology worldwide do not produce data about FRT searches, false positive cases, and what actions they have ignited, such as the number of stop-and-frisks or arrests.

With this context in mind, in this chapter, I will analyze how machine learning algorithms, specifically facial recognition algorithms, operate in the space of the production of 'order,' producing conditions of possibility for the formulation of practices in the gears of the criminal justice system. I argue that the trust placed in machine learning algorithm makes the production and stabilization of order and the production of norms and practices possible. To do that, I first turn my attention to the intertwining of algorithm rationalities with the practices of security and legal professionals (judges, prosecutors, public defenders, and lawyers), seeking to explore how these technologies have reshaped legal processes, making procedural safeguards fluid, as they produce ways of "proving" (evidence) and punishing.

In section 5.2 revolves a sample of concrete cases to explore how algorithmic rationality affects the possibilities of challenging evidence as it comes to constitute part of the routine of criminal justice professionals. Based on this discussion, I argue that FRT produces unequal distribution of security and rights, deepening the racialized, gendered and classed inscription of forms of violence. In this sense, I am less interested in identifying the 'legal exception', and more invested into analyzing the reconfigurations of security norms, especially criminal law, as they come to increasingly encounter FRT in the practices of such professional field.

After that, I focus on the practice of what the machine learning algorithm enables. This section aims to understand how these technologies disrupt and reshape the foundations of evidence admissibility, introducing new dynamics of power and knowledge into the legal sphere in USA. This approach critically reflects the intricate relationships between technology, law, and society, which is crucial for comprehending the complex interplay between truth, technology, and the norm in practice. I.e., when the evidences produced by FRT encounter the gears of the criminal justice system. Here, it is noteworthy that this research does not aim to provide legal analysis: rather, it explores the implications of algorithmic truth-telling on material-discursive practices and due process in line with STS studies and feminist critiques of technoscience. The emphasis is, thus, to understand where algorithms and norms intersect and how algorithmic discourses and rationalities are represented and contested in legal practice

Finally, the last section of the chapter revisits the arguments presented in the chapter. It supports the identification of the indeterminacy of the entangled practices of security and legal professionals with machine learning algorithms and how these raise complex questions about the possibilities of contestation. In doing so, this chapter demonstrates how algorithms actively participate in penal practices and how they shape the concept of 'doing justice.'

5.1. Encoding Justice: from leads for investigations to court

> *Law and technology both have the power to organize and impose order on society.*
>
> Nissenbaum, 2011, p. 1373.

Artificial intelligence has entered the premises of criminal justice systems allegedly to improve procedural justice and economy, as well as effectiveness and efficiency in decision making (ROBERTS; ZUCKERMAN, 2010; HILDEBRANDT, 2014). Previously argued, there is a growing discourse that algorithms deliver accuracy, objectivity, consistency, and "fairness", which is attractive to policymakers and the public. Such perception makes institutions seem "apolitical," as law and science to become potent trust generators (JASANOF, 2005, p.5). In the report "Using Artificial Intelligence to Address Criminal Justice Needs" (2019), the National Institute of Justice (NIJ) affirms the "potential [of algorithms]

to promote security and justice" for the criminal justice system. According to the report,

> Artificial intelligence has the potential to be a permanent part of our criminal justice ecosystem, providing investigative assistance and allowing criminal justice professionals to better maintain public safety (…) AI technologies offer the ability to overcome human errors and operate as experts (…) Every day holds the potential for new AI applications in criminal justice, paving the way for future possibilities to assist in the criminal justice system and ultimately improve public safety. Algorithms could also help prevent victims and potential offenders from falling into criminal pursuits and assist criminal justice professionals in safeguarding the public in ways never before imagined (RIGANO, 2019, p.8-9).

The proliferation of images of criminal events has brought automated facial recognition to the forefront of the Criminal Justice system in a big way (JACQUET; CHAMPOD, 2020). According to a Bureau of Justice Assistance U.S. Department of Justice report, over 80% of criminal cases involve video evidence[151]. The forensic use of images is divided into three main stages: investigative leads, intelligence, and evaluative (which can be used as relevant evidence in court). FRTs are framed as auxiliary mechanisms that can help security agencies and the court in investigating and fact-finding, reducing arbitrariness, systematizing the evidence process, and improving policing and trial efficiency (RIGANO, 2019).

As we can see, the text of the report highlights the previously unimagined possibilities that the use of algorithms can bring. It also highlights how these technologies extend the forms of cognition beyond the human, offering more precise information and even framing them as "experts." As Lynch and Jasanoff (1998) emphasize, legal practice has circumscribed expertise as a certified, reliable, and impartial account. According to Jasanoff (2003, p.159), "expertise is not so much found as made in the process of litigation or other forms of technical decision making."

In this way, expertise is a product of politics and culture in specific contexts that circumscribe what can be accepted as an accurate statement of fact (JASANOFF, 2003; 2005; LYNCH; JASANOFF, 1998). Thus, the expert's report

[151] BUREAU OF JUSTICE ASSISTANCE. Final Video Evidence Primer for Prosecutors. Available at: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/final-video-evidence-primer-for-prosecutors.pdf . Accessed on: March 15, 2024.

legitimizes and generates action in legal contexts. This framing of the NIJ report eloquently describes how algorithmic rationality has operated in the spaces of truth-telling construction within the machinery of the criminal justice system and how it has created conditions of possibility for the flexibility of procedural safeguards in practice. As noted in chapter 2, algorithmic reason helps us understand how these technologies are held together despite their heterogeneity in practice.

Science and technology aim to transmit "neutral," "objective," and more "effective" knowledge to deal with problems. Meanwhile, the intrinsic mission of the Criminal Legal System is to try to establish the truth of the facts and decide on the guilt or innocence of a person accused of committing a crime. As argued by Jasanoff and Lynch (1998) and Cole (2002), the boundaries between the production of 'scientific facts' and the 'truth of the facts' are significantly messier and fuzzier in practice. Tangled intra-actions of dispersed and heterogeneous material-discursive practices produce both law and science.

This section explores how security and legal professionals use FRT in practice and what this use makes possible regarding how evidence is generated and presented as 'good enough' from a lead of investigations to court. I aim to understand what makes the FRT reliable and preferable for "optimizing" justice from an identification mode from the algorithmic vision. The analysis focuses on the North American context but also provides insights into how models of security 'thinking and doing' (HACKING, 2006) have spread to other areas of experimentation. The dynamism in which the entangled multitude operates in the algorithmic practices of recognition can also be understood as one of indeterminacy.

There is an (im)possibility of defining the limits of what police work is and what algorithmic work is. According to Roberge and Castelle (2021, p.14), it is as if both man and machine are equally imperfect in their inability to control the potential space of intra-action between them fully. As Suchman et al. (2002) argue, whether a system works is neither obvious nor given. The perceived success or failure of its functioning depends as much on negotiated objectives as on the imperatives of science. So, the question that has pervaded this research continues to echo: how is trust established? Is it only through metrics such as accuracy and scores? As we have observed, certifications and tests are part of assembling

credibility, but there are other layers in which trust is distributed, established, and negotiated in the practice of agents.

The FRT establishes probable cause or individual proof of identification. As we noted in chapter 3, the issues of identifying and linking individuals to the bureaucratic traces kept on them and their past behaviors have constituted defining and elementary challenges for security practices in pursuit of maintaining order. Making this connection has been a significant driver of innovation in surveillance techniques and technologies and forensic science (COLE, 2002; LYON, 2006). As Jacquet and Champod (2020, p.5) point out, in forensic science, the aim of the scientist is to assess "the weight given to alternative propositions by the available evidence." More specifically, the calculation of the likelihood ratio, measured in the amount of information that can be offered (HACKING, 1990, p.107). However, it is crucial to acknowledge that despite attempts to reduce or neutralize error through standardization and technical-scientific development, no source of error can, in practice, be eliminated in this process of building evidence and identification (JASANOFF, 2006). This includes the potential for biases and errors in FRTs.

Identification is the key. FRTs draw elements of "recognition" from reliable biometric identification and drive them into identity deliberations required to resolve security issues. In part, this echoes the legal grounds that establish as legitimates that stop-and-frisk actions are carried out based on recognition, which then leads to investigations by law enforcement (GARVIE, 2022). However, a crucial difference arises when technology is integrated into the process. Initial recognition no longer derives from the discretionary exercise of the police officer, for example. Instead, officers make their decisions using algorithms. Here lies one major concern of this research: how do algorithms recognize and make perceptible to the analyst what an "anomaly" is? What are the conditions for security action through data evidence and its consequences, especially when they spill over into spaces like the courts? The singular action, an autonomous system's result (output) – the evidence of identity – is a multiplicity of human and algorithmic judgments, assumptions, limits, and probabilities. The algorithmic result is merely a fragile and contingent numerical probability (GILESPIE, 2014; AMOORE, 2020), so a small adjustment of the weights in the layers of the algorithm will change the output signal and, with it, the basis for the decision and security action.

In this way, technology plays an apparatus role (Barad, 2007) that cuts through how suspicion is generated and presented. As Fussey and Davies (2021, p.14) argue, "despite awareness of potential technological limitations," levels of trust and belief in these algorithms as "infallible" are high. In this sense, understanding what machine learning algorithms can do is just as important as understanding what professional fields believe these algorithms are capable of. In 2019, the report "Garbage in. Garbage out Face Recognition on Flawed Data," based on public records, pointed out that security agencies send all kinds of photos, expecting consistent and reliable results from facial recognition algorithms (GARVIE, 2019). There is a presumption of trust and built-in safeguards against errors, "yet this cannot be observed and proven under current operating conditions" (GARVIE, 2019, p.5).

Furthermore, the outputs of facial recognition algorithms acquire meaning within various practices of knowledge production and shared values about valid practices that are considered normatively adequate and legitimate. As Bigo (2006, p. 14-15) argues, constructing this epistemic space is a struggle between professionals and new forms of knowledge. For example, the meaning that professionals in law enforcement agencies give to the results and evidence produced by FRT is embedded in a particular "epistemic culture," so that the result of this evidence can acquire other meanings for legal operators. According to Pruss (2021), algorithmic methods are not only value-laden but also *introduce value* into how we reason about their application domain. For this reason, I will explore how police officers and judicial operators construct and understand the knowledge they receive through the algorithmic analysis of biometric data.

Machine learning algorithms' inherent pragmatism leads legal operators and law enforcement professionals to what is "useful" in each socio-technical context (ROBERGE; CASTELLE, 2021; AMOORE, 2019). The results must be capable of operationalization and simultaneously flexible enough to circulate in different contexts. In other words, algorithmic evidence has material-discursive effects that are constantly being (re)modeled. An almost paradoxical relationship exists between the attempt at norm and the variation and modulation that characterizes the algorithm and its practical use (ROUVROY; STIEGLER, 2016).

Thus, instead of serving as a machine for telling the truth about someone's identity, FRTs relate to each social and professional group's expectations and organizational and practical objectives. There is no uniform and absolute perception of what these technologies can achieve in criminal investigation: an investigator's expectations differ from the perceptions of developers or what is expected of judges, lawyers, jurors, or even defendants. The presence of FRT also brings different traditions, professional cultures, languages, and procedures into interaction. It immediately brings technical-scientific procedures and the law into a dialog – and tension (JASANOFF, 2006). As I have argued in this research, algorithms' results and the practices they make possible compose a mixture of administrative procedures, data, protocols, humans, and algorithms.

Leads for investigations

As we have seen, FRT has become popular with security agencies. However, there is little dissemination and production of reports and data that indicate its use and effectiveness as a security policy in practice. One example is that the New York Police Department, one of the largest in the US, has used the technology since 2011. However, it only disclosed in 2019 that its facial recognition system made 2,510 potential matches out of 9,850 requests that year. It did not disclose how many of these matches were false positives[152]. As noted in chapter 4, the NYPD also used Clearview AI's software in 2018, and there was no report on its use. Errors and false positives can be the ignition point for an expansion of forms of surveillance on individuals culminating in potentially unjust arrests. Errors are not abstract but material practices that can be violent. Furthermore, an arrest does not need to occur for a person or a community to suffer the damage of mistaken investigations generated from failures by and through facial recognition algorithms.

The use of TRF by US agencies in the last 20 years has occurred without fixed standards (GARVIE, 2022). Moreover, although specific guidelines and recommendations have been developed and disseminated, adherence to them remains entirely voluntary. In the absence of legislation, regulation, or jurisprudence to the contrary, it remains essentially the responsibility of each

[152] NEW YORK POLICE DEPARTMENT. Facial Recognition. Disponível em: https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page . Acesso em: 22 fev. 2024.

security agency at the various levels (local, state, and federal) to manage their system and each operator how to operate it. As Garvie's research (2022) shows, US security agencies state that they are not obliged to disclose information on the number of matches made by facial recognition. It is because, at least in theory, the results offered by FRT are used to produce leads for a complete investigation and are not the only ignition point for an arrest. However, there is a growing number of documented wrongful arrests in which algorithmic results accounted for virtually the entire investigation[153]. An important issue is that the use of TRF has led security professionals to disregard contradictory evidence and other data about the case, and the result generated by the algorithm has been represented as "overwhelming evidence" in the investigation (PRESS, 2023).

The "glue" connecting facial recognition evidence to a suspect is unclear; "probable cause" is broad and can frame different perceptions of what constitutes 'good enough' evidence. One example is that The New York City Police Department Patrol Guide[154] instructs law enforcement agents to conduct further investigation to determine if the “possible match” candidate is involved in an ongoing or past investigation to establish probable cause. According to the NYPD guide, "Additional investigative steps should be conducted in order to establish probable cause to arrest the Subject [sic] of the facial recognition search." (in GARVIE, 2019, n/p). In theory, officers appear to be given clear guidance on what additional evidence is needed to corroborate a possible facial recognition match.

However, there is no definition of how many additional investigative steps are required and to what extent they should be independent of the facial recognition process. Moreover, how much corroboration of a facial recognition match is enough before the police can make an arrest? How many people have been wrongly identified without the error being recognized as such?

These questions outline the lack of information, standard procedure, and regulation of the use of FRT by law enforcement agencies, an issue that we observe in a widespread way not only in the US. In this research, I have observed that there

[153] I will return to this point in section 5.3.
[154] NEW YORK POLICE DEPARTMENT. NYPD Facial Recognition Patrol Guide. Available at: https://www.nyc.gov/assets/nypd/downloads/pdf/nypd-facial-recognition-patrol-guide.pdf . Accessed on: February 22, 2024.

is no data on the practical use of facial recognition, how often it errors, and what is understood as the error in practice. It should be noted that errors can be framed in different ways, as can their acceptability (LISLE, 2017, p.2).

Security professionals shape and condition the use of algorithms at the same time these practices, forms of action, and ways of thinking are simultaneously shaped and conditioned by these technologies and the possibilities they bring (LATOUR, 1987; AMOORE, 2020; ARADAU; BLANKE, 2022; CRAWFORD, 2021). Information not only informs but also shapes (HEIDEGGER, 1997, p.182) how the police officer understands ‘suspicion’ (BRAYNE; CHRISTIN, 2020; FUSSEY; DAVIES, 2021). Several empirical questions concerning the operational uses of FRT arise in this dynamic. These include how the judgment of risks run by operators are framed by the information brought to their attention by the interface with the algorithm, the impact on subsequent operational judgments, the dynamic nature of human-computer interaction, and how this affects levels of risk and, therefore, willingness to intervene (FUSSEY; DAVIES, 2021).

In this sense, FRT can be operated in heterogeneous ways by different agents. There are reactive and adaptive processes (BRAYNE; CHRISTIN, 2020) that security professionals use to interact and adjust their practice with the algorithms. The discourse that came to associate these technologies with objectivity and efficiency obfuscates the fact that the algorithm does not operate separately in criminal investigations: it is entangled with human practices and the practical organizational context it is immersed in. Among the examples mentioned in the previous chapter, Clearview AI, relies on the input of a photo for the search and also on human "supervision" of the result, just as the result of an image can be used to reach other individuals and spaces as "targets" captured from image metadata. As algorithms expand, the modes of cognition and the possibility of action, agency, and responsibility diffuse in layers of practices and processes.

The relationship between the search made through the FRT and the crime can be tenuous. For example, someone who has liked a suspect's photo on Instagram or for whom "there was a basis to believe" that they are a witness to criminal activity. Clearview AI, for example, offers a range of possibilities for searching social networks and creating links and insights from the search image and metadata, such as location, date, time, hashtags, websites, and more. Moreover, we can

generate links between individuals and places from this metadata, as we saw in the example of Derrick Ingram's arrest. We see the expansion of likely suspects who need to be watched and neutralized to maintain order. This approach not only addresses the crime that has been committed but also aims to anticipate other potential crimes. It touches on a common concern shared by many efforts to manage future outcomes within the realm of security practices. As noted in chapter 3, pattern recognition and classification of people has been the modus operandi of various practices to control groups and individuals perceived as an "anomaly".

The previous chapter was described how a search with Clearview AI shows the security agent not just a single face but a "candidate list" of dozens, sometimes hundreds, of likely matches. Most of the returns, in other words, are false positives. The juxtaposition of many different faces, near and far from each other, in a more or less similar format produces an illusion of objectivity. It represents a form of 'trained judgment' (DASTON; GALISON, 2007), which produces a standardized method of observation that appears to eliminate the observer's subjective influence[155]. However, reviewing the list and deciding which candidate, if any, might be the correct match does not fall to an algorithm but to a person - a representative of authority whose qualifications in this area may be limited. We need to point out that the results can be flawed even with an accuracy level of 99.9%, as Clearview presented. The algorithm generates a probability of resemblance to a 'best estimate,' the accuracy of which will vary depending on the quality of the photograph, which can be compromised by factors such as lighting and camera angle, among others, as noted in chapters 2 and 3.

Although the expression "human in the loop" may seem to satisfy legal principles, as Suchman et al. (1999) argue, humans and technologies do not always act as expected. For instance, there are 41 policies that prescribe human supervision of government algorithms in the United States, but these are not accompanied by evidence and empirical data on how the "humans" have operated (GREEN, 2022). According to Green (2022), these policies that tries to brings human back in the looping can legitimize the use of algorithms even when they are related to

[155] One example of 'trained judgment' in scientific research, where using calibrated instruments and standardized procedures ensures that different researchers observing the same phenomenon will arrive at consistent and objective results, minimizing individual biases.

controversial cases and low accuracy in tests. The efficiency may still be lower because of the security agent's expertise. However, as the author argues, security professionals cannot perform the supervisory functions desired by legislators (GREEN, 2022). Instead of protecting against possible errors in algorithmic decision-making, human supervision policies provide a false sense of security when adopting algorithms.

Clearview AI offers an example of this. According to the company, Clearview AI is "lawful and constitutional" because "all searches result with independent investigations by the agencies."[156] The emphasis on human oversight as a protection mechanism allows two things: it promotes the algorithm, proclaiming that its capabilities exceed those of humans, while it defends human oversight as an indispensable component of credibility. This dual rhetoric allows the actors responsible for developing and implementing an algorithm to harbor goodwill towards the benefits of algorithms while simultaneously escaping accountability for the possible damage, errors, and injustices that algorithmic results can generate.

The Government Accountability Office's report on the use of FRT by the Department of Homeland Security and the Department of Justice law enforcement agencies showed that agents were using FRT without any training[157]. The FBI required some agents to take a 24-hour course, but the GAO revealed that only ten of the 196 officers with access to the technology had completed it[158]. In addition, the Scientific Working Group on Facial Identification recommends specific minimum training criteria for facial recognition analysts but only has 5 US states and 8 cities as its members[159]. Furthermore, some security agencies do not require any training, and the requirements for use and training (or lack thereof) are not publicly available (GARVIE et al., 2016).

---

[156] CLEARVIEW AI. Clearview 2.0. Available at: https://www.clearview.ai/clearview-2-0 . Accessed on: February 22, 2024.
[157] U.S. GOVERNMENT ACCOUNTABILITY OFFICE. Available at: https://www.gao.gov/products/gao-23-105607 . Accessed on: February 22, 2024.
[158] Ibid.
[159]Established in the late 1980s, U.S. and international forensic laboratories and professionals have collaborated in Scientific Working Groups (SWGs) to improve disciplinary practices and build consensus standards. Collecting and disseminating accurate information on applying FRT, facial recognition methodologies, and technologies. FACIAL IDENTIFICATION SCIENTIFIC WORKING GROUP (FISWG). Available at: https://www.fiswg.org/ . Accessed on: February 22, 2024

Given this context of widespread use by security agencies without information on its practicalities, the World Economic Forum, the United Nations Interregional Crime and Justice Research Institute, and Interpol published in 2022 the "good practices" report for the "responsible" use of facial recognition for law enforcement[160]. The report highlights the importance of standardized operating procedures by police officers concerning human rights, specific training, and transparency in actions and accountability practices. According to the report, the social and organizational elements are as essential as the technical ones when analyzing the efficiency of a law enforcement policy that includes technologies. This aspect is also present in the report "Law Enforcement: Facial Recognition Use Case Catalog" (2019) by the International Association of Chiefs of Police (IACP), in conjunction with the IJIS Institute, which developed guiding principles for the use of technology by security forces. The report includes four recommendations: fully informing the public, establishing parameters, publicizing effectiveness, and creating good practices and policies for use by police agencies[161]. However, I have observed that these good practices have not been adhered to and have not had widespread practical use (GARVIE, 2022).

In short, we are seeing a technical-legal apparatus that is becoming ubiquitous in the daily lives of security professionals. Most policies, procedures, and training guides made public do not educate security agents on what constitutes a sufficient quantity or quality of evidence, additional evidence to corroborate an identification, and how independent of facial recognition research the information evidence needs to be. Information on how security agencies have used this technology in practice is also scarce.

Although these professionals and the society in general lack the full picture of the functioning and the effects of FRT, the latter has been used by law enforcement agencies in a 'comfortable' way, even with flaws and controversies regarding the violation of fundamental rights such as the presumption of innocence,

[160] UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI). A Policy Framework for Responsible Limits on Facial Recognition. Available at: https://unicri.it/A-Policy-Framework-for-Responsible-Limits-on-Facial-Recognition . Accessed on: February 22, 2024.

[161] INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE (IACP). Facial Recognition Use Cases Report. Available at: https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf . Accessed on: February 22, 2024.

freedom of expression, and others. The use of FRT without any rules inverts the presumption of innocence, requiring us to continually prove our innocence - our "nothing to hide" status - in order to avoid a charge of wrongdoing. Some places where technology has been experimented with and used in security practice do not even limit facial recognition searches to criminal suspects. In practice, FRT has justified discriminatory and violent actions, in which (in)security is enacted and negotiated. It is to this discussion that we now turn to.

Criminal courts

Abstract legal and administrative principles (the letter of the law) and the everyday practices of legal professionals are often dissociated in a "loose coupling," where there is a significant amount of authority and discretion in which the legal norm is done in practice (BRAYNE; CHRISTIN, 2020). As Lynch and Cole (2017) point out, with the implementation of technical-scientific apparatuses, legal operators adjust their practices due to new standards and metrics.

As we have analyzed, security agencies have widely used evidence derived from facial recognition for stop-and-frisk investigations and criminal proceedings. However, the subjects who are 'recognized' and accused based on this evidence are often deprived of the opportunity to challenge it. Exploring the potential impact of technology on law enforcement and the criminal justice system, the National Association of Criminal Defense Lawyers (NACDS, 2019) poses the question: "If the technology is admitted as evidence in court, and if the results are admitted, what do defendants need to challenge that evidence?" (NACDS, 2019, p. 10). To engage with this problem, it is important to analyze the specifics of how facial recognition evidence came to be admitted in courts, allowing for the reconfiguration of the practices characterizing the criminal justice system.

The widespread use of FRT emerges as a legal challenge in practice; in particular, there is the challenge of recognizing cases in which facial recognition technology is used as a lead for investigation and evidence to link the prosecution. This is because, as we noted earlier, its use is often not disclosed for the defense, nor is it clear how the suspect was identified in the first place. The same way, it is unclear whether the evidence produced by facial recognition may have produced a confirmation bias by the eyewitness, for example. Suggestive procedures can occur

when authorities signal to witnesses that facial recognition has been used and that the perpetrator must be present in the photographs presented, thus increasing the chances that the wrong individual will be selected (GARVIE, 2022). Although eyewitness identification is among the most common types of evidence admitted in court, it is also one of the most problematic due to the high misidentification rate. A recent study by the Innocence Project found that 75% of wrongful convictions in the US occurred in involved eyewitness misidentification[162]. As Bronx public defender Kaitlin Jackson argues,

> what I believe is happening most of the time is that the police are getting a zeroing in on a target and then they are taking either that person or more likely the photo and doing some kind of identification procedure with an actual eyewitness and then once you get that case in court you may only see that there was an eyewitness identification it's very likely that your case will look just like a standard eyewitness identification case there is no real you know bullet proof method to figure out that you have a facial recognition case(…) that point is this is the human identification really new evidence or is it just confirmation of what the machine has already determined[163].

According to Jasanoff (2006, p. 329), the expectations of legal professionals must be worked out in the particular types of propositions, representations, and material objects that the law considers admissible to establish which party is the "most plausible singer of the story". The growing belief in the field of legal professionals (jurists, lawyers, judges, and others) that scientific evidence is reliable and that science offers insights that would otherwise be hidden in a judicial investigation is part of a need to make complex social issues "visible and interpretable" in court (JASANOFF, 2006). In this research, we have seen how FRT entangle with that professional field through promises of rendering the justice system more efficient, thereby contributing to 'better justice'. Nevertheless, there is also a 'what a shame' discourse, given the vanishing possibility of challenging the evidence provided by such algorithms (ROUVROY; STIEGLER, 2016, p.7). The

[162] INNOCENCE PROJECT. How Eyewitness Misidentification Can Send Innocent People to Prison. Available at: https://innocenceproject.org/how-eyewitness-misidentification-can-send-innocent-people-to-prison/ . Accessed on: February 22, 2024.
[163] NACDLVIDEO. Face-Off: Recognizing and Challenging the Use of Facial Recognition Technology [webinar]. YouTube, August 20, 2019. Available at: https://www.youtube.com/watch?v=s4k3BLcH6OI (from 39:17 to 57:27). Accessed on: February 22, 2024.

current quest for objectivity, the attempt to be closer to the "fact itself," has created limits to interpretations and doubt, and this produces "problems in the legal metabolism" (ROUVROY; STIEGLER, 2016, p.8) in practice.

Criminal trials are and have always been practical exercises in reasoning under uncertainty. In those stages, evidence rationally authorizes or shapes inferential conclusions (Robert; Stockdale, 2018). Legal decisions depend not so much on whether something is true or false as on the plausibility of the story told as true, on the relevance of the evidence to the case, and on how much it contributes to the strength and quality of the evidence (JASANOFF, 2006). Uncertainty and certainty are not mutually exclusive in legal reasoning and are closely intertwined in probabilistic reasoning. Indeed, "probability is not new to the law" (HACKING, 1975, p. 86). The law has its own functional rules and ways of making the ‘real’ come to existence. For example, the confession of a crime in court is framed as truth not according to the consistency of the relationship between what was said and what happened but by the fact that the law gives a truth value to the confession itself (ROUVROY; STIEGLER, 2016).

According to Haack (2014, p.47), to understand "degrees of certainty" applied in law, we must look not to mathematical probabilistic rationality but to epistemology. Legal standards of evidence are best understood in terms of the degree to which the evidence presented must justify the conclusion (of the defendant's guilt or liability) for a case to be brought. As analyzed in chapter 2, throughout its history, the concept of probability has two aspects: it links both with the notion of a degree of certainty guaranteed by evidence and with the notion of a tendency to produce stable probabilities. The distinction between speculation and uncertainty is only possible to the extent that the law's probabilistic language of "reasonable suspicion" and "sufficiently credible evidence" is reformulated in the language of a scientific method. As the algorithmic results (output) achieve the status of a real and objective description, they vest with efficiency and objectivity claims that would otherwise be more complex and uncertain to interpret.

In short, the degree of certainty depends on the quality of evidence – material evidence and reasons – regarding what is being enunciated. Evidence can support an assertion, weaken it, or do neither. The better the independent certainty of the reasons supporting a claim, the more plausible the claim of truthfulness will

be; and the better the independent certainty of the reasons undermining a claim, the less justified it will be (HAACK, 2014, p.50). In line with this, how much support a particular piece of evidence gives to a conclusion depends on how much the addition of that evidence contributes to the explanatory integration of the whole.

The value and quality of forensic evidence can vary significantly depending on the context. What may be considered 'good evidence' for justice in one situation might be useless in another. Additionally, technical evidence must meet specific criteria to satisfy the epistemological requirements of the law[164]. These requirements involve principles of logic, reasoning, and scientific methodology to evaluate whether the evidence meets the necessary threshold to be considered trustworthy and convincing in a legal context. This demonstrates that the concepts of evidence quality and degree of assurance are complex, nuanced, multidimensional, and context-dependent.

Moreover, the law has its own institutional needs and constraints, and these are largely aimed at ensuring that justice is done in each individual case (JASANOFF, 2006, p.329). The widespread use of FRT emerges as a legal challenge in practice; in particular, there is the challenge of recognizing cases in which facial recognition technology is used as a lead for investigation and evidence to linking to the prosecution. This is because FRT are not mentioned in the case files as the tool that led to identification, nor is it clear how the suspect was identified in the first place, leaving open the bias that may have been produced by the eyewitness, for example. Those biases can occur when authorities signal to witnesses that facial recognition has been used and that the perpetrator must be present in the photographs presented, thus increasing the chances that the wrong individual will be selected (GARVIE, 2022).

In addition to the challenge of knowing whether that facial recognition is being used and how it is being used in court cases, there is widespread ignorance of how machine learning algorithms work and the risk that they "will not get it right" every time (NUTTER, 2019, p.925). Moreover, because the law is not designed to interrogate forensic practices that are not going to be introduced in court, if FRT is

[164] I will discuss in the next section.

the ignition point of an investigation but is anchored by other evidence, the technology itself is unlikely to be questioned. As emphasized by lawyer Jackson,

> the difficulty with facial recognition is that right now we're not seeing prosecutors trying to actually introduce this stuff in court right they're relying on that other evidence often that identification that was made by an eyewitness after the facial recognition match happened[165].

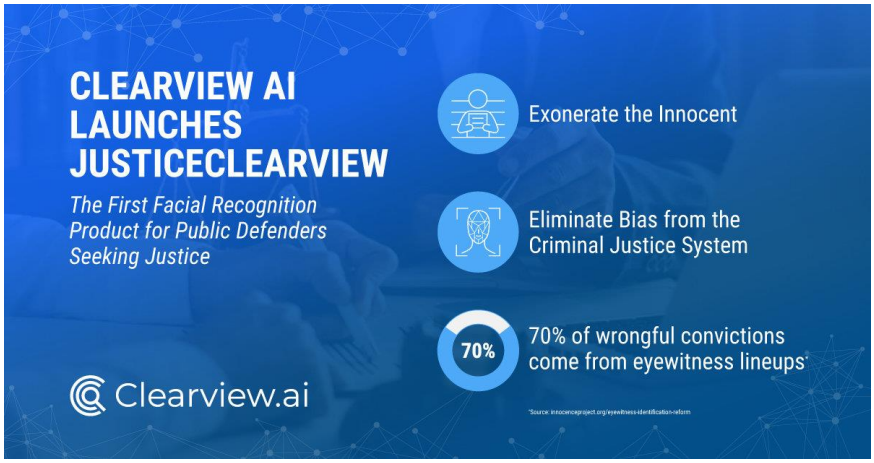
For this reason, a challenge that has been raised is how to challenge the admissibility of the facial recognition algorithm based on its method of producing evidence in court, which we will analyze in more detail in the next section. To take the simplest cases, there are a number of questions about the reliability of facial recognition technology evidence, about the limitation in its accuracy given the conditions of the photos being analyzed, for example.

Debates about how to challenge FRT, its use in the courts, and the challenges of using algorithmic tools in the justice system have taken centerstage in the US. In this same context, Clearview, which has been offering its system to law enforcement agencies since 2018, launched, in 2022, Justice Clearview, the "first facial recognition tool for public defenders," a platform that "ensures justice is available to all."[166] The company's corporate pitch is to offer "the same state-of-the-art technology" being used by enforcement agencies, so that the criminal justice system can become "fair and just."[167] According to Ton-That, "[p]eople would think about the use of technology differently if public defenders had access to it."[168] As we have seen, the company has remodeled and circulated its algorithm in different practice spaces, but with the discourse of "improving" and making existing practices more objective, with the promise of "eliminating bias from the Criminal Justice System."

---

[165] Ibid, (45:48).
[166] CLEARVIEW AI. Clearview AI Launches JusticeClearview: First Facial Recognition Product for Public Defenders Seeking Justice. Available at: https://www.clearview.ai/press-room/clearview-ai-launches-justiceclearview-first-facial-recognition-product-for-public-defenders-seeking-justice . Accessed on: February 22, 2024.
[167] Ibid.
[168] CLEARVIEW AI. Available at: https://www.clearview.ai/public-defenders . Accessed on: February 22, 2024.

Figure 18. JusticeClearview



Source: Clearview AI.

In the context of finalizing this research, the use of FRT by defenders is not yet widespread, and the only company that offers it is Clearview AI. There is criticism of the errors and biases of these systems and resistance due to ethical issues surrounding the broader use of Clearview tools[169].

However, there are advocates of the possibility of the tool being used to exonerate a falsely accused innocent person, in other words, the possibility of "doing justice." For example, Jonathan Lyon, coordinator of the National Association for Public Defense, points out that he has an "enormous interest in the technology" because the "tool would be useful, especially for tracking down eyewitnesses"[170], as I observed in the case presented in chapter 4. For Jerome Greco of the Legal Aid Society, the use of FRT to produce defense evidence "is a rare situation in which most defense attorneys would want to use it," but this is being used as marketing by the company to "try to resist the negative publicity that Clearview AI has about its tool and how it is being used by law enforcement."[171] Jumara Musa, director of the National Association of Criminal Defense Lawyers,

[169] THE NEW YORK TIMES. Available at: https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html . Accessed on: February 22, 2024.
[170] Ibid.
[171] THE NEW YORK TIMES. Available at: https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html. Accessed on: February 22, 2024.

says, "[y]ou do not solve problems in a broken criminal legal system by applying technology to them."[172] The use of facial recognition by defenders and defense attorneys as evidence remains a limited and controversial area, as discussed in detail in Section 5.3. However, this research reveals how these technologies are intra-actively reshaping the practices of legal professionals.

As the NIJ report points out, the expanded use of FRT in the criminal justice system operates at rates that exceed human capacity, but, as I have emphasized, they are not without errors and bugs. There is a promotion of the algorithm, claiming it surpasses human capabilities, while simultaneously defending it from scrutiny by highlighting the (supposed) security of human oversight. What we see is not the overcoming or rupture of a way of doing and thinking about security and justice but a rationality that produces new conditions of possibility for policing, investigation, and "truth-telling" in court, even if, as we will discuss in the next section, there is no methodological standardization of the use of technology as evidence in the courts.

It may be that many of those arrested based on questionable facial recognition searches did commit the crime they were accused. Nevertheless, there is the possibility that they did not – that the facial recognition system identified the wrong person – without additional, independent police investigation and sufficient access to evidence by the defense. Instead of protocols, norms, and the inseparability that guides FRT evidence from investigative leads to use in court, I observed a messy tangle of human and non-human practices, organizational infrastructures, bureaucracies, norms, protocols, and data.

Furthermore, the impact of the "matches" on the individuals who are materialized through the practice of FRT is often unclear. In addition to the lack of data on the use of FRT, when errors are not recorded, they are not considered or understood as such within the penal system. The people who are investigated, arrested, and charged with crimes they did not commit will bear errors and failures in practice. They often do not have access to essential information, such as what sparked their arrest was an FRT, which would guarantee access to a fair trial.

[172] Ibid.

As the discussion to follow will show, we are not only accepting the possibility of errors as part of the machine learning, but also accepting the failure of the criminal justice system to protect due process and the fundamental rights of these individuals.

5.2. Algorithmic errors and failures in practice: differentiated distribution of (in)security and rights

> *If the mission is for the technology to get it wrong frequently, we would predict that we are getting a lot more incorrect identifications, you would assume that facial recognition in criminal cases is resulting in more positive identifications, right? But you could assume that it's very likely that it's resulting in more true positives and more false positives and we need to find out how often those positives are false.*
>
> Kaitlin Jackson, Bronx's Public Defender[173]

As we saw in the previous section, FRTs are increasingly present in the Criminal Justice System. Identification failure has historically been a factor of insecurity, both in the production of knowledge about the suspect and in the production of unjust arrests (GARVIE, 2022; PUGLIESE, 2010). The very development of biometrics operates in parallel with the search for improvements in security practices by producing a recognizable and traceable subject, as I analyzed in chapter 3. FRT "illuminates the already present problem of locating a clear account of a knowable human subject" (AMOORE, 2020, p.136), as well as the production of an 'actionable target' (AMOORE; HALEY, 2017). This thesis has paid attention to the performative effects of how 'recognizing' constitutes, structures, and alters actions and social worlds. The output of an FRT is never true or false but a practical proposition that can be infinitely recombined (AMOORE, 2020; CRAWFORD, 2021).

In this sense, the algorithmic practices of FRT serve to formalize and codify the social practice of policing in a way that calls into question the fundamental legal frameworks that underpin long-standing controls over these practices (BRAYNE, 2021, p.835). According to Deleuze (1995, p.175), the machines themselves explain

[173] NACDLVIDEO. Face-Off: Recognizing and Challenging the Use of Facial Recognition Technology [webinar]. YouTube, [data de publicação não especificada]. Available at: https://www.youtube.com/watch?v=s4k3BLcH6OI (at 56:18). Accessed on: February 22, 2024.

nothing. Instead, “you have to analyze the collective apparatuses of which the machines are only one component” (DELEUZE, 1995, p.175). From this perspective, several ethical and political questions arise from the growing power of algorithmic facial recognition in security practices and how it relaxes rights and produces norms.

As analyzed above, errors are not bugs or side effects solved by optimizing the machine learning algorithm: they are part of the materialization of material-discursive practices that the algorithm has made possible. The different ways of making mistakes, false positives, and false negatives directly impact the likelihood of an innocent person being investigated, or even arrested, for a crime they did not commit. When a system gets the identification wrong, it will still produce a list of candidates with possible matches. Even if the algorithm does not recognize the face, it makes another form of knowledge production possible. This is why we will now analyze some public cases of facial recognition errors and failures and how the distributed and composite forms of authorship that draw divisions of anomaly can produce violations of rights, spaces of exclusion, unequal distribution of security, and reinforcement of social hierarchies. These cases are a sample of an unknown totality of cases that are underreported.

In April 2018, Bronx, New York, public defender Kaitlin Jackson was tasked with defending a man accused (the accused's name and characteristics have been kept confidential) of stealing a pair of socks from a TJ Maxx store (JOHSON, 2022). The accused claimed he was unable to commit the crime because he was in a hospital, approximately one kilometer from the location, at the time of the theft, awaiting the birth of his child, which occurred about an hour after the incident. The public defender was baffled by how the police managed to identify and capture her client months after the incident (JOHSON, 2022). After contacting the Bronx District Attorney's office, she was informed that the identification was made through a security camera photo using facial recognition technology.

The only witness to the theft, a store security guard, later revealed that the police sent him a photo of the accused, asking via text message if he was responsible for the crime. Jackson questioned the legitimacy of the identification method and the chain of custody of the image, which prompted the judge to call a hearing to assess whether the identification method was inappropriately suggestive. The

defender points out that she could not suppress the identification or the facial recognition evidence discredited by the prosecution. According to her, "they have an unshakeable faith that the software does not make mistakes."[174] Soon after, as Jackson reported, her client was offered a deal: to admit guilt to a lesser offense in exchange for a sentence already considered served. The client, who had been detained for approximately six months, accepted the offer; after all, "he just wanted to get on with his life"[175]. He pleaded guilty to something he did not do, and the evidence given on recognizance was not challenged or destabilized as good enough probable cause for arrest.

In this context, public defender Ketlin Jackson wrote an article to the National Association of Criminal Defense Lawyers presenting strategies for dealing with facial recognition evidence, especially when the use of the tool is unclear[176]. According to the document, if the basis of suspicion is unclear, photos or videos are listed as evidence, and an eyewitness identifies your client, these aspects may suggest that facial recognition has been used. In addition, the document points out that lawyers should request supporting materials for an investigation, including a list of all candidates returned by a facial recognition system and the reliability scores assigned to them. This request was unsuccessful in the case presented above, and the defendant accepted a plea bargain with the prosecution.

In February 2019, Nijeer Parks was charged with theft following the escape. Parks was accused of robbing a hotel gift store in Woodbridge, New Jersey, and trying to run over a police officer with a rental car (JOHSON, 2022). Woodbridge police then sent a blurred and shadowed image of the fake driver's license photo (used to rent the identified car) to an out-of-state investigator, who ran the image through a facial recognition system. The investigator informed the officers that Nijeer Parks was a "high profile comparison" (a term apparently made up out of

[174] NEW YORK MAGAZINE. The Future of Facial Recognition in America. Available at: https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html . Accessed on: February 22, 2024.
[175] WIRED. How Wrongful Arrests Based on AI Derailed Three Men's Lives. Available at: https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ . Accessed on: February 22, 2024.
[176] NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS (NACDL). Challenging Facial Recognition Software in Criminal Cases. Available at: https://www.nacdl.org/Article/July2019-ChallengingFacialRecognitionSoftwareinCri . Accessed on: February 22, 2024.

whole cloth by the officers)[177]. According to the case documents, the image and the input from the facial recognition search were blurred, and the sides and lower third were shaded. In other words, the image used by the police was of poor quality. When it was run through the FRT program, the image had been manipulated several times significantly distorting its original version[178]. As we saw in chapters 2 and 3, even with image quality as close to "ideal" as possible – in terms of brightness, angle, and quality of definition – facial recognition systems operate more or less accurately in different demographic groups, especially Black people, as in Parks' case.

In addition to that, there is the risk of error introduced by human review of FRT search results. When a human analyst does an initial review of the hundreds of candidates generated by FRT, the analyst's cognitive biases can compound the racial biases in the FRT-generated candidate list and introduce errors (GARVIE, 2022). As we have analyzed from research and reports in chapter 2, operators tend to trust the results of the machine learning algorithm due to "automation bias." Human analysts may assume that there is a precise enough match in the algorithmic results, even when there is not. It should be noted that the relationship will have more or less operator adherence in each context.

As discussed in the previous section, the lack of scrutiny surrounding evidence produced by facial recognition tools necessitates the inclusion of additional evidence to corroborate the investigation and establish probable cause for a subject's arrest. The documents about Parks' arrest, when Sgt. Tapia (in charge of the case) filled out a form requesting the use of FRT; the form warned that it was a "possible match" from an FRT search

> should only be considered an investigative lead. Further investigation is required to confirm a possible match through other information and/or evidence corroborated by the investigation. INVESTIGATIVE LEAD, NOT PROBABLE CAUSE TO

[177] AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY. Amicus curiae brief of the American Civil Liberties Union and the American Civil Liberties Union of New Jersey in support of plaintiff's opposition to defendants' motion for summary judgment. Available at: https://www.aclu.org/wp-content/uploads/2024/01/113-1.-ACLU-ACLU-NJ-Amicus-Brief-Filed.pdf . Accessed on: February 22, 2024.
[178] Ibid.

> MAKE AN ARREST. ECF No. 109-5 at 290 (Defs' Ex. T) (emphasis in original)[179].

Such warnings to the police were standard during the facial recognition search in this case (2019). As we analyzed in section 5.1, the International Association of Chiefs of Police and the US Department of Justice indicated in their primary documents that this should be standard practice.

However, far from heeding this warning, the police, in this case, treated a single facial recognition search result not as an investigative lead that required independent corroboration but as a definitive match. Nijeer Parks 'looked' like the suspect based on the comparison made by the algorithm. An important point is that he was elsewhere during the crime. He was in a pharmacy fifty kilometers away, making a money transfer via Western Union (HILL, 2020). When Parks received notification of the arrest, he went voluntarily to understand why he was being charged, and, even though he presented an alibi, he was arrested and spent US$5,000 in legal fees before being released at a custody hearing (HILL, 2020). The Woodbridge police arrested Parks and kept him in jail for ten days, although they could have confirmed that he was not near Woodbridge at the time of the incident if other stages of the investigation had been carried out.

Despite his innocence, Nijeer Parks initially considered a plea bargain for fear of going to trial on charges of assault, theft, and evasion and being a repeat offender on other drug charges. Losing at trial would result in a longer sentence, the maximum being 25 years, compared to accepting a plea bargain (Hill, 2021). According to Parks,

> That is when I started beating myself up, like a plea bargain might not be a bad thing, even if I didn't do it, because with a trial longer and me being a convicted felon, my time is doubled[180].

Parks was acquitted almost a year later and spent ten days in jail (JOHSON, 2022). It's important to note that in his acquittal, the focus of the questions went more towards his alibi (not being in the place where the crime was committed), than

[179] Ibid.
[180] WIRED. How Wrongful Arrests Based on AI Derailed Three Men's Lives. Available at: https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ . Accessed on: February 22, 2024

towards the identification made by the FRT. In March 2021, Parks filed a lawsuit in federal court in New Jersey against the director of the Woodbridge Police Department, other local authorities, and Idemia, the manufacturer of the facial recognition system that identified him, alleging false arrest, private imprisonment, violation of his rights, improper search and seizure and disproportionate punishment (JOHSON, 2021). The lawsuit alleges that the police did not use traditional investigative techniques, such as submitting a photo of Parks to a personal interview or a photo list for witnesses, among other investigative mechanisms.

Furthermore, the lawsuit also claims that the police failed to obtain DNA evidence or fingerprints left at the scene by the suspect, which could have eliminated Parks as a suspect. A trial date has not yet been set. Parks' case calls our attention because the algorithm has been considered as a “good-enough” evidence for his accusation. When asked about the evidence used to charge him in an interview, Nijeer Parks says: "It was not any evidence. (…) It is just a picture that the computer said he looked like me"[181].

FRT use collected data to extract patterns from a population, replacing a normalized template ('deductive logic') with curves modulating normality ('inferential potential' and 'experimentation'). As we observed in chapters 2 and 3, on the one hand, these technologies are still linked to a disciplinary diagram that uses the face as a mechanism for individualization. On the other hand, however, these technologies no longer depend on a direct link between identity and likeness through the way they learn and operate. In this context, what counts "are the relationships between the data, which are only infra-individual fragments, partial and impersonal reflections of everyday existences that data mining allows to be correlated on a supra-individual level, but which does not indicate anything greater than the individual " (ROUVROY; BERNS, 2013, p.27).

This problem is also seen in the case of Michel Oliver, a 25-year-old black man who was arrested in Ferndale, Michigan, during a traffic stop in July 2019. The arrest came two months after Detroit police issued a warrant for his arrest for

[181] YOUTUBE. He was innocent. But a facial recognition 'match' got this Black man arrested. Available at: https://www.youtube.com/watch?v=nGStQVeCYuw (at 2:50). Accessed on: February 22, 2024.

allegedly taking a smartphone from a teacher who was recording a fight outside a school and throwing it on the ground. Oliver was at work when the crime occurred[182]. Detroit police used FRT to identify Oliver based on images from the recorded video. After the algorithm recognized him, the investigation and case file added the identification of the teacher, an eyewitness. What connected Oliver to the crime was his degree of "similarity" to the suspect according to the facial recognition algorithm.

In an interview, Oliver's public defender, Patrick Nyenhuis, said that, upon making acquaintance at the custody hearing, he quickly realized that his client did not look like the man in the video. Oliver has several tattoos, while the person in the video has no visible tattoos[183]. In addition, the defender pointed out that the detective in charge of the case took "shortcuts," including not questioning Oliver or reviewing the video evidence of the incident before his arrest. Wayne County prosecutors agreed with the defense's allegations and dropped the charges. The Wayne County Prosecutor's Office pointed out that "current protocol requires a supervisor to review all evidence in a facial recognition case prior to a charging decision. There must also be other evidence to corroborate the allegations in order to charge someone."[184]

In addition to pointing out that the prosecutor's office "knows of no other cases of false identification with the use of face recognition technology," Detroit Police Chief James Craig said he believed "strongly in facial recognition software,"[185] but "if we just used the technology by itself to identify someone, I would say 96% of the time they would be incorrectly identified"[186]. In his speech, the Chief of Police reinforced the human presence in the loop and said that good

[182] DETROIT FREE PRESS. Facial Recognition Technology Leads to Wrongful Arrests in Detroit. Available at: https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ . Accessed on: February 22, 2024.
[183] WXYZ DETROIT. Facial Recognition Technology Led to this Detroiter's Wrongful Arrest. Available at: https://www.wxyz.com/news/region/detroit/facial-recognition-technology-led-to-this-detroiters-wrongful-arrest . Accessed on: February 22, 2024.
[184] DETROIT FREE PRESS. Facial Recognition Technology Leads to Wrongful Arrests in Detroit. Available at: https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ . Accessed on: February 22, 2024.
[185] DETROIT FREE PRESS. Facial Recognition Technology Leads to Wrongful Arrests in Detroit. Available at: https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ . Accessed on: February 22, 2024.
[186] Ibid.

investigative practice does not count only with algorithmic evidence for igniting an arrest.

In this case, no evidence was considered to corroborate the arrest warrant other than the evidence produced by the FRT and the corroborating eyewitness account. The police department acknowledged that the lead investigator did not carry out the due diligence he should have before making the arrest[187]. According to Andrew Rutebuka, head of the Criminal Intelligence Unit that used the technology, "We sent the image to the detective. But from there, the detective has to go out and look at the photo and compare it with any other information"[188]. The investigators are trained to follow up the facts, as they would in any other case, such as confirming the person's whereabouts at the time the crime took place or comparing any other records. As we noted earlier, the presence of someone on a list of candidates for facial recognition alone is not a sufficient basis for proceeding with a witness identification procedure and establishing a substantial basis for believing a 'reasonable suspicion' that the suspect committed the crime and should therefore be presented to the eyewitness. What we have seen in this research is that "reasonable suspicion" can be a very broad term, but one with concrete and deep implications for the innocent lives matched under that "reasonability".

Although he was acquitted, Oliver pointed out how this mistake at the TRF unfolded into different processes of violence in his life. In an interview, he pointed out that:

> I have a son, I have my family, I have my little house, I pay all my bills, so when I was arrested and lost my job, it was as if everything had collapsed, as if everything had gone down the drain[189].

Michel Oliver had his mobility restricted, lost his job, and acquired financial and psychological problems. As we have seen, algorithmic errors and failures create conditions of possibility for violation of rights. These practices affect the lives of those on whom the data is processed. To challenge and reverse the data, Oliver filed

[187] Ibid.
[188] WIRED. How Wrongful Arrests Based on AI Derailed Three Men's Lives. Available at: https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ . Accessed on: February 22, 2024.
[189] Ibid.

a lawsuit against the city of Detroit for the error in his arrest. The lawsuit accuses the Detroit Police Department of using

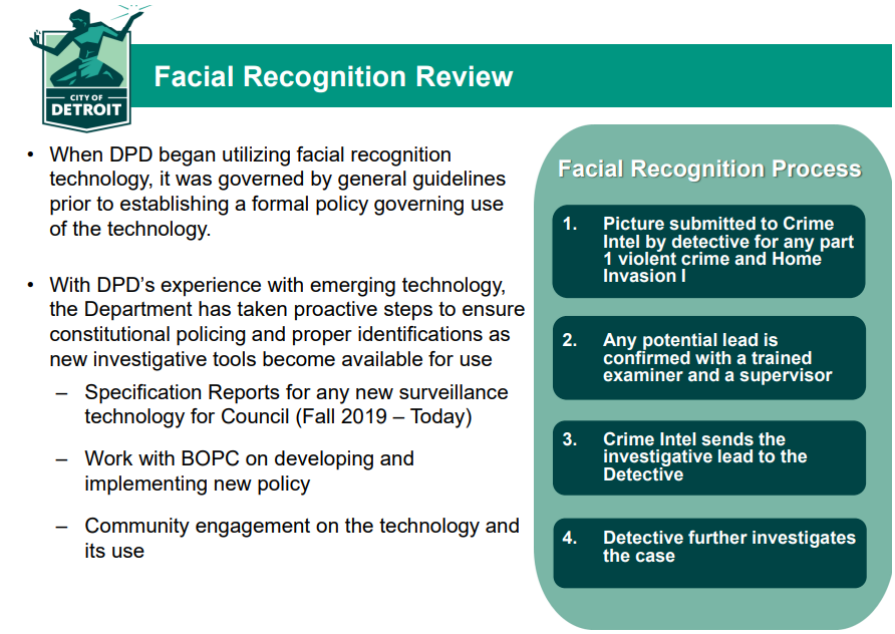
> flawed facial recognition technology, knowing that the science of facial recognition has a substantial error rate among black and brown ethnic people, which would lead to the wrongful arrest and incarceration of people in this ethnic demographic[190].

In the lawsuit, Oliver seeks an order preventing Detroit police from using facial recognition technology until biases and low accuracy are resolved in the technology's performance. Moreover, the lawsuit cautions that if facial recognition software is used in an investigation, investigating officers are required to inform judges reviewing arrest warrants that the quality of an image can affect the accuracy of their results. Oliver's lawyer, David Robinson, asks that the police reveal how many images the facial recognition program returned other than Oliver's. He also seeks records on the accuracy of the facial recognition program, as well as on the accuracy of the technology in identifying black people in a city where the majority of the population is black or brown[191].

The case is still on trial. Since Oliver's arrest and the widening public debate about the use of FRTs, the Detroit Police Department has revised its policy on the use of facial recognition software. Since 2020, FRT can only be used in cases of violent crime, and the police department has shared how the algorithmic evidence formatting flow operates, as we can see in the image below.

Figure 19. Face Recognition Review, Detroit Police Department

[190] Oliver v. Detroit, City of et al (2020). Available at: https://dockets.justia.com/docket/michigan/miedce/2:2020cv12711/349847 . Accessed on: February 22, 2024.
[191] YOUTUBE. He was innocent. But a facial recognition 'match' got this Black man arrested. Available at: https://www.youtube.com/watch?v=nGStQVeCYuw. Accessed on: February 22, 2024.



Fonte: DPD, 2020[192]

This "new" protocol did not prevent other failures in using facial recognition algorithms. In January 2020, Robert Williams, a 43-year-old black man, was arrested for robbing a watch store in Detroit, Michigan. The robbery took place in October 2018. Although he had not visited the store for several years, he was arrested as a suspect in the presence of his two daughters. The Detroit police department used facial recognition technology from the company DataWorkPlus to identify him as a suspect through surveillance camera images, the quality of which, according to the case report, "was grainy," as well as having low light, an angle that does not focus, and showing a person who is also obscured by the use of a cap, as we can see in the following image. Williams was identified as a "possible match" (Hill, 2023, p.227). The image of Williams that purportedly matched the probe image was an expired driver's license photo. Mr. Williams has a newer driver's license photo on file with the State of Michigan, but that newer image was not a likely match for the suspect[193]. Furthermore, in the arrest warrant issued for Williams, there was no "critical information about the deficiencies in the

[192] CITY OF DETROIT. Facial Recognition and Project Green Light. Available at: https://detroitmi.gov/sites/detroitmi.localhost/files/2020-08/Facial%20Recog%20and%20Project%20Green%20Light.pdf . Accessed on: February 22, 2024.

[193] AMERICAN CIVIL LIBERTIES UNION OF MICHIGAN. Facial Recognition Leads to False Arrest - Williams v. City of Detroit - Complaint. Available at: https://www.aclumich.org/sites/default/files/field_documents/facial_recognition_leads_to_false_arrest_-_williams_v_city_of_detroit_-_complaint.pdf . Accessed on: February 22, 2024.

investigation and how facial recognition technology was used."[194] As we have observed, there are no instructions on what type of input image meets a minimum standard to be used as evidence.

Figure 20. Photo used to identify Robert Williams in the investigation

Source: Case Robert Julian-Borchak Williams v. City of Detroit – Complaint. 2020 (p.16)

As we can see in Williams' case, after being arrested, the police officer observed that the algorithm's facial identification had failed. The report of the Williams vs. City of Detroit case (2020, p.34) also adds the information that DNA samples and records of his palm prints were collected in addition to his return to prison. It highlights not only the issue of misidentification but also how an individual's biometric data can be retained, used, and reinserted into the machinery of the criminal justice system, creating a lasting trail that potentially affects a person's life after release. As Pugliese (2010, p. 95) writes, “[a]Against the intentionality or will of the subject, the body-bit of a subject, once converted into a biometric template, will effectively reveal the identity of the clandestine or concealed subject; the body offers itself despite the subject."

What happened to Williams is not an isolated incident; it raises essential questions about the credibility and trust in FRTs, the practices of collecting and storing biometric data, and the implications of reusing this data. Once this data enters the machinery of the Criminal Justice System, it can influence future

[194] Ibid.

decisions and possibly expose the individual to further encounters with the justice system. As the number of intra-actions, a person has with the police force increases, the more likely they are to be detained and, consequently, the greater the risk of being wrongly identified in criminal proceedings.

Furthermore, the machine error produced material effects: Robert was held in custody for 30 hours and was released on bail of US$1,000. He said in an interview: "The technology was so reliable that they didn't even do any investigative work to find the person. Nobody ever asked me from any police department, 'Where were you on the day of the crime? In the absence of simple investigations, such as whether Robert was there, based solely on the results offered by the FRT, Detective Donald Bussa presented the photo to an eyewitness, a store clerk. It should be noted that the crime took place in 2018, and as noted, there are critical questions about susceptible distortions and suggestibility depending on different factors (CROZIER, 2023). "Bussa's investigation impermissibly relies on facial recognition technology."[195]

Williams's case was the first case of error in the use of facial recognition tools in US law enforcement practices with national notoriety. Since Williams' arrest, other cases have emerged (such as those presented by the Bronx public defender), and unsurprisingly, the people wrongly identified were black. Williams, in a text published on June 24, 2020, in The Washington Post, points out:

> I keep thinking about how lucky I was to have spent only one night in jail — as traumatizing as it was. Many black people won't be so lucky. My family and I don't want to live with that fear. I don't want anyone to live with that fear.[196]

These recent examples of the application of facial recognition technology by the police raise questions not only about the development and use of the technology by law enforcement agencies but also about how mistakes and failures in practice are affecting what is understood as due process and the safeguards of rights, such as the presumption of innocence. Like Nejjar Parks and Michel Oliver,

[195] WIRED. How Wrongful Arrests Based on AI Derailed Three Men's Lives. Available at: https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ . Accessed on: February 22, 2024.
[196] THE WASHINGTON POST. I was wrongfully arrested because of facial recognition. Why are police allowed to use this technology? Available at: https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrongfully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/ . Accessed on: February 22, 2024.

Robert Williams is suing the police department over his arrest. He has also engaged in movements to ban the use of technology in law enforcement practices in conjunction with the ACLU[197]. It is worth noting that Williams' case sparked the circulation of previous cases. The lawsuit seeks compensation, greater transparency about the use of facial recognition, and an end to the use of facial recognition technology by the Detroit Police Department[198]. As Phil Mayor, one of the ACLU lawyers in the case, points out

> It is deeply troubling that the Detroit Police Department knows the devastating consequences of using faulty facial recognition technology as a basis for arresting someone and continues to rely on it anyway[199].

Robert Williams' case was neither the first nor the last. On February 16, 2023, in Detroit, Pocha Woodruff, who at the time was eight months pregnant, received a warrant for her arrest on charges of burglary. Six officers from the Detroit Police Department were at her house to make the arrest. According to the case documents Porcha Woodruff v. City of Detroit (2023), she was implicated as a suspect through a list of photos shown to the robbery victim, following a match generated by a facial recognition algorithm. On the day Woodruff was arrested, she and her fiancé asked the officers to check the warrant to confirm that the woman who committed the crime was pregnant, which they refused to do, the lawsuit alleges[200]. She was arrested at her home in front of her children and was taken in handcuffs to the Detroit Detention Center.

According to the report by investigator LaShauntia Oliver, in charge of the case, after extracting images from a gas station surveillance camera video, the image was used as input for an FRT search and then presented to the robbery victim,

---

[197] MIT TECHNOLOGY REVIEW. Robert Williams's lawsuit could change facial recognition forever. Available at: https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/ . Accessed on: February 22, 2024.

[198] Case Robert Julian-Borchak Williams vs. City of Detroit (2020, p.50).

[199] AMERICAN CIVIL LIBERTIES UNION (ACLU). After Third Wrongful Arrest, ACLU Slams Detroit Police Department for Continuing to Use Faulty Facial Recognition Technology. Available at: https://www.aclu.org/press-releases/after-third-wrongful-arrest-aclu-slams-detroit-police-department-for-continuing-to-use-faulty-facial-recognition-technology . Accessed on: February 22, 2024.

[200] NBC NEWS. Detroit woman sues city after being falsely arrested while 8 months pregnant due to facial recognition. Available at: https://www.nbcnews.com/news/us-news/detroit-woman-sues-city-falsely-arrested-8-months-pregnant-due-facial-rcna98447 . Accessed on: February 22, 2024.

who identified Porcha as a suspect[201]. Woodruff was held for 11 hours and only released on $100,000 bail. She went straight to the hospital, where she was diagnosed with dehydration. According to Porcha, in an interview with the New York Times: "I was having contractions in the cell. My back was giving me sharp pains. I was having spasms. I think I was probably having a panic attack. I was suffering, sitting on those concrete benches."[202]

A month later, the Wayne County prosecutor closed the case for insufficient evidence[203]. Her lawyers used the Fourth Amendment of the U.S. Constitution, which guarantees "no warrants shall issue, but upon probable cause, supported by oath or affirmation." Porcha also filed a civil suit for damages caused by her arrest. Moreover, as in the other cases we have seen, it is also a form of litigation for greater transparency and the limitation of using FRT more broadly by law enforcement agencies. In an interview, she highlights how violent and traumatizing her experience with the penal system was, not only for her but for her entire family. Porcha's case also happened in Detroit after the Michel Oliver and Robert Williams cases.

The continued use and trust, even amid errors that generated national repercussions, demonstrates how algorithmic reasoning builds trust among security professionals and produces a practice of normative ordering in an abductive and adaptive way through data. Algorithmic output produces an actionable target that would otherwise not be possible, such as the case of Porcha – how could an eight-month pregnant woman steal a car? – and materializes the effects of insecurity in the lives of people who are perceived as targets of security attention, as happened with all the cases presented.

> You know, so, with that being said, that was a traumatizing experience. It still is. My kids are afraid. I'm afraid. The police get beside me or behind me, I go into a panic mode instantly. My kids go in a panic mode instantly. My kids thought I would have been shot. They've seen police

[201]DOCUMENTCLOUD. Woodruff v. Detroit Complaint. Available at: https://s3.documentcloud.org/documents/23901036/woodruff-v-detroit-complaint.pdf . Accessed on: February 22, 2024

[202] THE NEW YORK TIMES. Facial Recognition Leads to False Arrest. Available at: https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html . Accessed on: February 22, 2024.

[203] CNN. Detroit facial recognition technology leads to false arrest lawsuit. Available at: https://edition.cnn.com/2023/08/07/us/detroit-facial-recognition-technology-false-arrest-lawsuit/index.html . Accessed on: February 22, 2024.

> officers on my doorstep, you know, guns on their hips. They're saying I'm into carjacking, and that's a — you know, armed robbery and carjacking, that's a serious crime[204].

There are consequences to being implicated in the intra-active practices of producing security knowledge by and through FRT. However, experimentation, and therefore failure, has been normalized; after all, as James White, Detroit's chief of police, said when interviewed about the case, "I have no reason to conclude at this time that there has been any violation of the DPD's facial recognition policy."[205]

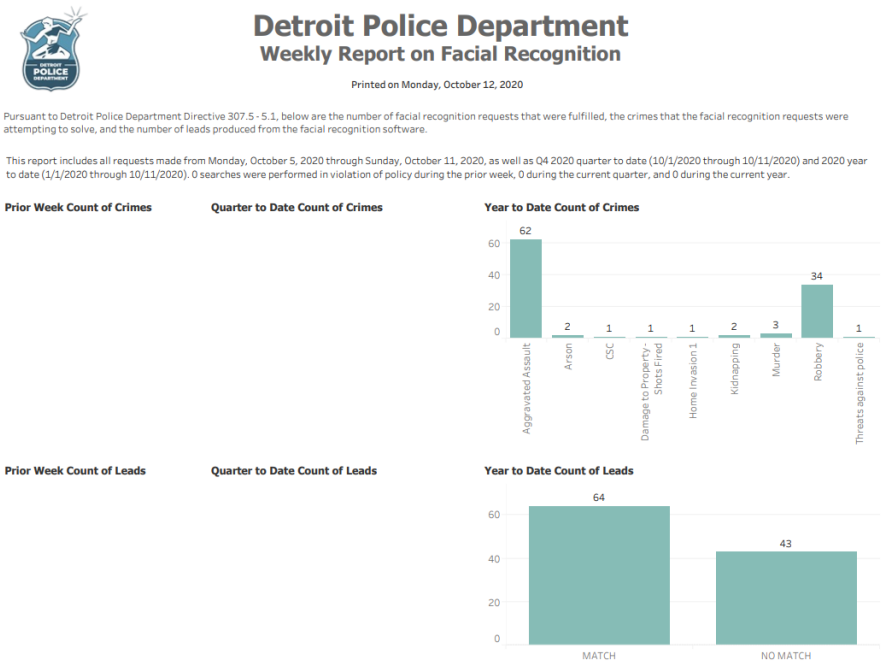
Furthermore, the Detroit cases and their public repercussions contributed to the DPD presenting data samples on how it used FRT weekly on its website. Data from the first report in October 2020 showed that FRT was used on black people in 97% of cases[206], reflecting the reinforcement of a profile of suspicion that has been historically constructed. In addition, as we can see in the figure below, there is a large number of "no matches," i.e., searches that did not result in any "leads" for investigation.

In 2022, before Porcha was arrested, the DPD published a TRF use directive to establish the "acceptable use" of the technology. This document states: "If a match is found through DPD's Facial Recognition process, it shall be considered an investigative lead, and the requesting investigator shall continue a thorough and comprehensive investigation."[207] Some elements show that despite the errors, flaws, and limitations, the TRF continues to be used in Detroit, not because it is perfect, but because it is practical and feeds back into a way of thinking and doing security that conveniently categories of suspicion. Thus, error and failure are residual, and we have observed the displacement of questions of what is considered an error and of truth. The entanglement of algorithmic practices, data, legal, and security

[204] DEMOCRACY NOW!. Interview conducted by Amy Goodman on August 9, 2023. Available at: https://www.democracynow.org/2023/8/9/porcha_woodruff_false_facial_recognition_arrest . Accessed on: February 22, 2024.
[205] CNN. Facial recognition technology leads to false arrest in Detroit. Available at: https://edition.cnn.com/2023/08/10/us/facial-recognition-technology-detroit-false-arrest/index.html . Accessed on: February 22, 2024.
[206] CITY OF DETROIT. DPD Facial Recognition. Available at: https://detroitmi.gov/government/boards/board-police-commissioners/dpd-facial-recognition . Accessed on: February 22, 2024.
[207] CITY OF DETROIT. Facial Recognition - Under BOPC Review March 2023. Available at: https://detroitmi.gov/sites/detroitmi.localhost/files/2023-03/307.5%20Facial%20Recognition%20-%20%20Under%20BOPC%20Review%20March%202023_0.pdf . Accessed on: February 22, 2024.

professionals has operated across the boundaries of the productive acceptance of errors.

Figure 21. Detroit Police Department: Weekly Report on Facial Recognition



Source: DPD Report on Facial Recognition Usage 100520.

Although the DPD is still using the technology widely, the debate about failure and error has produced a pause, a reshaping, and an adjustment in how algorithmic practices have been framed and has discompose the idea of the "infallible" tool. As we have observed in this research, the credibility of the facial recognition algorithm is "assembled" through a fluid, dispersed, contested, and open process of material-discursive practices and not a fixed characteristic of the specific algorithm. For this reason, algorithmic error and failure can be productive methodologies that can overturn the typical assumption that algorithmic reason should lead to greater objectivity and precision in the practices of security and law. The DPD use case reinforces how, even amid flaws, algorithms are still good enough for thinking and doing security.

The examples presented so far are the cases that have circulated and received media coverage about the errors in the FRTs. What we have come across is that there is a problem and a challenge when the algorithm works – as we saw in the examples at the beginning of this chapter with recognizing demonstrators – but also when the algorithm goes wrong. Here, I return to the specific algorithm I am delving

into in this thesis: Clearview AI. As we saw in chapter 4, Clearview AI's corporate discourse frames it as the most accurate facial recognition tool in the USA, and the most extensive database available has an algorithm with high accuracy. However, it is not perfect; it is perfectible. It is not just a question of accuracy: once a face is recognized in the data and reaches a certain threshold of similarity, suspicion becomes sufficient for police action, even without other evidence, making the legal norm more flexible. At the time of this research, only one case of Clearview's algorithm error has been recorded. Nevertheless, the company does not recognize any degree of responsibility for its algorithm in the specific case (HILL, 2023) — the case of Randal Quran Raid.

Randal is a 29-year-old black man arrested in November 2022. He was arrested in Atlanta for shoplifting in Louisiana. The police report from DeKalb County in Atlanta, where he was arrested, points out that the arrest came about through a random check of Mr. Reid's license plate that revealed outstanding arrest warrants by Louisiana police[208]. According to the New York Times report of March 31, 2023, it was not clear from the arrest warrant how police came to identify him as a robbery suspect. According to…, this information was only possible after "paying thousands of dollars to find out."[209] Randal's arrest was made possible through correspondence from the TRF, and no official document mentioned the use of technology as a "lead" or means of identification. Here, we can observe a relaxation of the penal procedure that lets people subject to arrest be informed about what led them there. The warrant states only that he was identified from a "reliable source."

Figure 22. Statement by Detective Andrew Bartholomew requesting a warrant for the arrest of Randal Quran Raid

[208] THE NEW YORK TIMES. Facial recognition leads to false arrests. Available at: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html . Accessed on: February 22, 2024.
[209] Ibid.

Detective Bartholomew reviewed the surveillance video and was able to utilize still photographs from the video to identify three of the four suspects.

Detective Bartholomew was advised by a credible source, the heavyset black male from June 22, 2022, was Randal Reid. Detective Bartholomew conducted a search of the name, which revealed a DMV photograph of a Randal Quran Reid (B/M, DOB: [redacted], which appeared to match the description of the suspect from the surveillance video.

Detective Bartholomew requests an arrest warrant for the body of Randal Quran Reid (B/M, DOB: [redacted] for the charges of ten counts of RS14:67.16 C(1) Identity Theft $1000 or more, ten counts of RS14:71.1 Bank Fraud, and one count of RS14:67 B(2) Theft $5000-24999.

Source: HILL; MAC, 2023.

According to The New York Times documents, the Louisiana Police Department has been using Clearview AI technology since 2019. The company's CEO, Hoan Ton-That, has reinforced in interviews about the case and even before it, as we saw in the previous chapter, that an arrest should not be based solely on a facial recognition search and that the tool's goal is to offer "leads." This discourse shifts the blame onto humans rather than the possible errors of the tool.

However, this relationship is more complex: as I have seen, algorithmic practices are part of broader arrangements. In September 2023, Raid Quran filed a lawsuit accusing the misusing the FRT in his criminal case. The suit names Jefferson Parish Sherriff, Joseph Lopinto, and Detective Andrew Bartholomew as defendants[210]. Clearview AI is not named in the lawsuit. It is worth noting that, as I observed in chapter 4, Clearview AI has been circulating through adherence adjustments and has participated in important legal debates that can set precedents, such as the use of the First Amendment to protect and legitimize its algorithm and data scraping method, as well as limiting processes for scrutinizing and challenging its algorithm in court, for example.

In an interview, Randal states, "I would say I lost faith in the justice system to know that you could be locked up for something that you've never done in a place that you've never been to as well."[211] Contact with the criminal justice system at all levels (from contact with the police officer to incarceration) affects how individuals interact with and perceive other institutions (BRAYNE, 2014). Reid Quran was imprisoned for six days. He had never been to New Orleans, but he looked like the

[210] THE NEW YORK TIMES. Facial Recognition Leads to False Arrests. Available at: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html . Accessed on: February 22, 2024.
[211] ABC NEWS. Black man alleges wrongful arrest after misuse of facial recognition technology. Available at: https://www.youtube.com/watch?v=12HFqRMGAxc (at 3:04). Accessed on: February 22, 2024.

suspect in a surveillance camera video, and the algorithm pointed him out as a likely suspect. In the research on the documents, I observed that no other forms of investigation in the case file ignited the arrest warrant. According to the sheriff of Jefferson, the New Orleans County where the case took place, "as soon as we realized it was not him, we moved mountains to get him out of jail."[212] A judge in Louisiana issued the warrant, and the crime was investigated by the police there. He was only released when a judge in that jurisdiction freed him[213].

The delimitation of what is acceptable or not as a "side effect" of the failure has been normalized. The case also sheds light on the fact that if "thousands of dollars" had not been spent on hiring law firms with capillarity in both jurisdictions to verify what led to his arrest, perhaps this case would not have been framed as an error in using FRT. It highlights how the production of non-knowledge, the absence of information, limits the possibilities of recognizing an error and the algorithmic practice itself.

5.3. Truth-telling: unpacking the admissibility of facial recognition evidence

Evidence is something that points beyond itself.

Ian Hacking, 2006, p.37

The primary function of law is to do justice (JASANOFF, 2006). 'Doing justice' requires a complex balancing of multiple considerations in an analytical framework that keeps social contexts in sight while constructing compelling narratives of cause and blame (JASANOFF, 2006). So, when science and technology enter the courtroom, they should do so in complement to the law's need to tell credible stories (LYNCH, 2013; COLE, 2015). As we analyzed in chapter 2, machine learning algorithms operate in a specific mode of truth production. As an apparatus (BARAD, 2007), algorithms structure knowledge about someone's identity; they "show" reality and intervene in it.

[212] THE NEW YORK TIMES. Facial Recognition Leads to False Arrests. Available at: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html . Accessed on: February 22, 2024.
[213] THE NEW YORK TIMES. Facial Recognition Leads to False Arrests. Available at: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html . Accessed on: February 22, 2024.

This section addresses the debate on admissibility and how, even though FRTs have not yet been classified as "technical evidence" according to existing methodologies, they are good enough to support a process in Criminal Justice. It is how the norm is also being materialized in practice. The aim of this section is twofold: both to examine the most fundamental changes in the production of knowledge in Criminal Justice environments that occur as a result of the stabilization of the trust and credibility placed in facial recognition algorithms and to think about how these technologies are operating in practice, making the established processes of the legitimacy of the criminal process more flexible. It is more flexible in this context because, even though a standardized methodology for assessing the admissibility of FRT evidence has not yet been established, FRT continues to be utilized at various stages of the legal process, as we observed in the cases presented in the previous sections.

For FRT results to be used in court, there is a need for trust in the processes that led to that evidence being materialized, in addition to the adjudication of the operator, the security professional. Reliability is the "cornerstone of judicial evidence" (ROBERTS; STOCKDALE, 2018, p.4), although approaching reliability from a 'logical angle' is often neglected in public debates (JASANOFF, 2006, p.332). There are times when scientific evidence can be considered good enough to be admitted to court even if it does not meet the standards of scientific certainty. Courts, as well as algorithm development laboratories, can therefore be considered experimental spaces in which statements about reality are constructed, presented, tested, held accountable to standards and eventually determined to be reliable or unreliable (JASANOFF, 2005). So, how do we frame the trust placed in facial recognition evidence in the courts?

A hallmark of modern legal systems is that they aspire to rationality in their conclusions and judgments (LYNCH, 2009; JASANOFF, 2003; 2005; 2006). Verdicts in criminal trials should be based on reliable evidence and verified to a required standard of admissibility and credibility of proof (ROBERTS; STOCKDALE, 2018, p.42). Evidence-based sentencing promotes algorithms as an objective and empirically sound rational technology to improve decision-making (HANNAH-MOFFAT, 2013, p.271). Although the admissibility and validity of

evidence in its strictest sense is based on proof in principle, reliability also means achieving epistemic validity, a value beyond scientific validity (WIENROTH, 2020), as noted in the previous section when dealing with degrees of certainty.

With the increased use of facial recognition technologies in recent decades, as we have seen in the previous chapters, the reliability of these algorithms has been a significant focus of research in the academic, governmental, and commercial arenas, such as the NIST tests and benchmarks. An attempt to standardize, establish technical levels, and mitigate the "black box effect" – the non-knowledge and opacity that algorithmic processes and choices produce. These tests, combined with other empirical research, highlight two main ways in which algorithms can impact the reliability of a facial recognition search by security officers: the performance of different algorithms and the performance of algorithms on different subjects and operational situations (GARVIE, 2022; FUSSEY; DAVIES, 2021). The diversity of algorithms available and the lack of standardization in their use and regulation also generate different possible results.

As we have seen in previous chapters, these technologies have been criticized numerous times. As security and legal professionals focus on the algorithm(s) involved in the organizational configuration(s), they risk privileging the algorithm in the ongoing formation of the organization. In other words, the algorithm becomes part of the solution to justice. However, when it is a problem, the solution is the technical improvement of the algorithm and the attempt to standardize its practices. Thus, the response to criticism of the use of algorithmic technologies in criminal justice has been to attempt to create norms, rules, and formalization within algorithmic governance to tame the exceptionality of algorithmic practices by bureaucratizing decisions. Although there is no standardization, the more certifications, tests, and widespread use by other agencies an algorithm has, the more it is framed as efficient and reliable, as I observed in the previous chapter on stabilizing Clearview AI's credibility. The more reliable an algorithm is, the more it will circulate and be perceived as appropriate to influence decisions and practices.

It should be noted that the methods and production of evidence for investigative purposes demand a lower 'scientific standard' than those that produce

evidence used in court (GARVIE, 2022; JASANOFF, 2006). In this way, security agencies have greater scope in the investigative phase for approaches that are not based on well-established science because there is an assumption that investigative leads are confirmed with other evidence before a search or arrest is carried out. For example, with eyewitness testimony. Even though, as I have observed, in practice, the FRT results can represent the totality of evidence. The process of adjudicating FRT evidence in investigation and policing is done by the security agents who operate the system and assess the credibility of the result presented. The 'human in the loop' would, in theory, mitigate identification errors and failures, as we noted in the previous section.

In law, the "veracity" of testimonial evidence must be explicitly demonstrated, establishing a chain of custody from the scene of the action to the court (JASANOFF, 2005; COLE, 2005; MACHADO; GRANJA, 2020). FRTs, like other algorithmic evidence, do not yet have a delimited chain of custody in the legal systems in which these systems are being used. The opacity of algorithmic processes can represent a barrier to their use as evidence in court due to the difficulty in establishing expertise and explaining processes (JACQUET; CHAMPOD, 2020). Besides, for a forensic technique to be considered scientifically valid, it must be subjected to empirical tests under conditions that represent its operational use (JACQUET; CHAMPOD, 2020). Despite the numerous studies published in the last decade evaluating facial recognition accuracy rates, there is no exhaustive research and testing on the reliability of facial recognition as a representative sample of how security agents use. In this sense, there is room for subjectivity and conjecture, cognitive bias, low-quality or manipulated evidence, and underperforming technology to be presented in the courts (GARVIE, 2022).

According to the National Research Council[214] (2009, p.107), "Much forensic evidence is introduced in criminal trials without any meaningful scientific validation, determination of error rates, or reliability testing to explain the limitations of the discipline." The use of this evidence has been distinct, with low

[214] OFFICE OF JUSTICE PROGRAMS. Available at: https://www.ojp.gov/pdffiles1/nij/grants/228091.pdf Accessed on: February 22, 2024.

clarity in the processes, without an established chain of custody. This has not hindered the increasing use of FRT in courts, nevertheless.

As mentioned earlier, TRF evidence is theoretically an investigative lead corroborated with evidence admissible in court, as a testimony of an eyewitness. Some legal professionals have used FRT as an analogy for examining a different forensic technique (i.e., as a composite piece of evidence with others) and basing a way of analyzing forensic evidence on methodologies that are already standardized. Others have considered facial recognition to be equivalent to a new scientific technique that would allow for the revision of a previous determination of the use scientific methods in court (think of another methodological form of standardization) (HADDAD, 2020; GARVIE, 2022).

An emblematic case is *Florida v. Lynch*[215]. In 2019, the Florida state appeals court ruled that Willie Allen Lynch, a black man convicted in 2016 for selling drugs, was denied the right to see photos of other suspects identified by the facial recognition algorithm search that led to his arrest[216]. The police, in this case, also relied on an eyewitness account, which the defense contested, along with Lynch's criminal record, to identify him as the culprit. During his trial, Lynch claimed that he had been incorrectly identified, alleging that the facial recognition system may have made a mistake and was misleading the officers[217].

Lynch was sentenced to eight years in prison. One point to note in this case is that if Lynch's defense had not taken it upon themselves to request depositions and file handwritten motions, he might never have known about the facial recognition algorithm's role in his identification and arrest[218]. Due process of law requires that prosecutors give jurors and defendants full access to this information to ensure that defendants can present their cases and that judges and jurors can make

[215] ELECTRONIC FRONTIER FOUNDATION. Lynch v. Florida Amicus Brief. Available at: https://www.eff.org/pt-br/document/lynch-v-florida-amicus-brief . Accessed on: February 22, 2024.
[216] Ibid.
[217] Ibid.
[218] AMERICAN CIVIL LIBERTIES UNION. Florida Using Facial Recognition to Convict People. Available at: https://www.aclu.org/news/privacy-technology/florida-using-facial-recognition-convict-people . Accessed on: February 22, 2024.

fully informed decisions on serious questions of guilt and innocence. As we have seen, these fundamental principles have been relaxed in practice with FRT.

Despite being one of the first public cases in which the defendant litigated his identification by facial recognition, there is no discussion of whether or not the evidence produced by the facial recognition algorithm is admissible. The state of Florida indicated in its brief that it did not intend to introduce facial recognition evidence in court, partly due to concerns that it would not pass the Daubert admissibility standard (an existing standard for scientific-technical evidence)[219].

For scientific evidence to function as a legal norm, the notion of scientific reliability must be translated into tests that judges can follow (JASANOFF, 2017). The case *Daubert v. Merrell Dow Pharmaceuticals, Inc*[220] (HC No. 740.431/DF 2022/0133629-9) is considered a gatekeeper for the admissibility of algorithmic evidence in the courts and the US Supreme Court decision. The case concerned the teratogenic nature of Bendectin, which the defendant company produced[221]. The scientific evidence presented by the plaintiffs was considered weak, as it consisted of a review of epidemiological studies that had not been published in a peer-reviewed journal. The evidence was rejected. The case reached the Supreme Court, which was called upon to rule on a question of law, namely whether or not the precedent of the Frye test (the standard for admissibility of technical or scientific evidence)[222] had been overcome in light of the Federal Rules of Evidence, a new statute on evidentiary law that had been passed in 1975 (CHENG, 2022; HADDAD, 2020).

For the US Supreme Court, however relevant a piece of scientific evidence may be, it should not be admitted if it does not achieve a minimum degree of

[219] Ibid. Lynch's sentence continued even after the appeal because other evidence corroborated the evidence produced by the facial recognition that led to his identification.
[220] JUSTIA. Supreme Court case 509 U.S. 579. Available at: https://supreme.justia.com/cases/federal/us/509/579/ . Accessed on: February 22, 2024.
[221] CORNELL LAW SCHOOL. Available at: https://www.law.cornell.edu/supct/html/92-102.ZS.html . Accessed on: February 22, 2024.
[222] The Frye standard, or the Frye standard, is a legal standard used to determine the admissibility of scientific evidence in court. It originated in the 1923 case of Frye v. United States and requires that scientific tests or procedures are only admissible as evidence when they have gained general acceptance in the specific field to which they pertain. The test ensures that expert opinion based on a scientific technique is only admissible when the technique is generally accepted as reliable in the relevant scientific community (GARVIE, 2022; JACQUET; CHAMPOD, 2020).

epistemic reliability. A piece of evidence is relevant to a given evidential hypothesis if its inclusion contributes to increasing or decreasing its explanatory integration. In other words, it contributes to the true and reliable assertion of facts necessary for "doing justice" (JASANOFF, 2005, p.79). In the decision establishing the Daubert standard, the Supreme Court emphasized the crucial role of judges as gatekeepers, determining which scientific evidence should be admitted into the case and which should be rejected. In other words, judges should be able to distinguish 'good' from 'bad' science through method (LYNCH; COLE, 2015; JASANOAFF, 2005).

The Daubert v. Merrell Dow Pharmaceuticals, Inc. case was a landmark decision, the first case in which the United States Supreme Court directly addressed a standard of admissibility of technical-scientific evidence and methods in court. The ruling influenced many countries internationally (JASANOFF, 2005) because it drew attention to wrongful convictions based on unreliable expert evidence. In recent years, detailed reliability requirements have been introduced in academia, forensics, and standardization bodies (SOMMER, 2010). According to Jasanoff (2005), the procedural change brought about by this precedent is part of a more profound epistemological shift. This 'shift' has repositioned the grounds for the admissibility of evidence and opened up a broader debate about the procedures through which law and science regulate their relationship with each other and, thus, how to deal with the search for legal redress for failures of science and technology. For Jasanoff (2005, p.40),

> the demands signaled disenchantment in contemporary America with the capacity of the law to resolve the multiple technical disputes of modernity and a concomitant acceptance of the imagined clarity, certainty, and rationality of science.

The U.S. Supreme Court ruled through the case that a trial judge must evaluate whether expert testimony or scientific-technical evidence is based on valid scientific reasoning that can be applied to the facts presented in that particular case. This decision was adopted from Rule 702 of the Federal Rules of Evidence (FRE), a congressional bill enacted in 1975[223]. In 2000, the United States Congress

[223] CORNELL LAW SCHOOL. Daubert Standard. Available at: https://www.law.cornell.edu/wex/daubert_standard . Accessed on: February 22, 2024.

amended the FRE to match the language of the Daubert decision, thus making Daubert the new standard in Federal Courts when deciding the admissibility of science-based evidence[224].

As we have seen, this has been the gatekeeper methodology for the admissibility of technical-scientific evidence, which is why I will analyze the conditions of possibility for framing FRT evidence. Important to note, at the time of writing this dissertation, I have not seen specific cases that challenge the admissibility of the facial recognition algorithm based on this methodology in a straightforward manner. According to Garvie (2002) and Haddad (2020), the path has been Daubert when thinking about fitting algorithmic evidence into existing methodologies. I will unpack each aspect of Daubert's admissibility concerning the FRT. According to the Daubert standard, five factors must be considered to determine whether the methodology is valid and whether the evidence can be considered admissible or not in court.

1. Whether the theory/technique in question can be or has been **tested**.
2. Whether the theory/technique has been subjected to **peer review** and publication.
3. Whether the **potential error rate** of the theory/technique is known.
4. The existence and maintenance of **standards** and controls.
5. Whether the theory/technique is **widely accepted** within a relevant scientific context.

The testability. Facial recognition technology is easily testable through experiments; this step is part of developing the machine learning algorithm. However, as discussed in Chapters 2 and 3, facial recognition algorithms do not operate in isolation; they are a tangled multitude of practices. Thus, the results of the same algorithm can vary considerably depending on the space in which it is experimented. As a practical matter, facial recognition is (un)testable in its entirety. The human, the data, the training of the algorithms, and the range of skills of a given operator mean that the universe of variables is potentially infinite.

[224] OFFICE OF JUSTICE PROGRAMS. Available at: https://www.ojp.gov/pdffiles1/nij/225333.pdf . Accessed on: February 22, 2024.

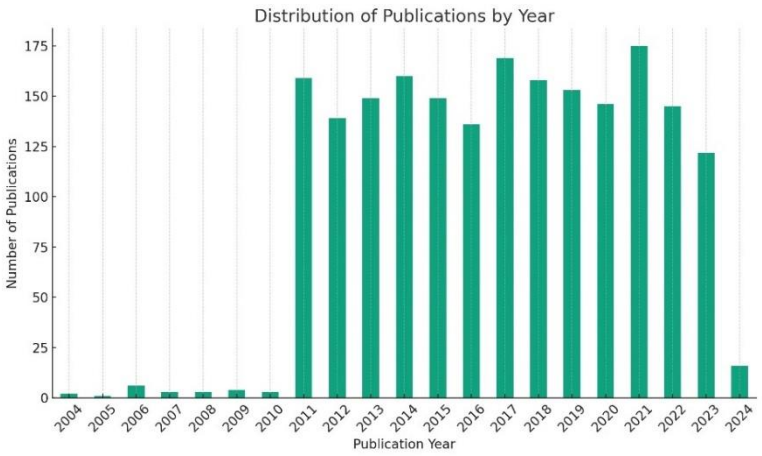
Although, as noted above, FRTs are subject to testing[225]. There are several proprietary and third-party algorithms in different security agencies, and as there is no established standard, each one can be tested independently. Thus, as a scientific method, FRT lacks an evaluation of how it is currently used by law enforcement or protocols that require research: operating within the methodological parameters of the studies that have been carried out and presenting results that guarantee its operation within these standards. Therefore, the NIST tests, for example, are about the reliability of facial recognition prototypes, not the technology used and implemented.

About peer review and publications as conditions of admissibility of FRT. There is no doubt that there is abundant literature on facial recognition technology. The scientific community has written about this technology and explored its uses and applications. For peer review, the report by The President's Council of Advisors on Science and Technology (2016) suggests that fundamental validity should only be considered established when two such studies have been published and substantially agree with each other in their findings. In a search carried out on the IEEE Xplorer database[226], which has a comprehensive collection of articles on engineering, computer science, and related areas, for the keyword "face recognition" and with the filter "method"; "methodology" and "standard" we have the following results in the graph below. This search illustrates, albeit to a limited extent in a single database, the volume of articles on face recognition methods and methodologies that have undergone peer review and been published. However, the reference to the peer review method may be insufficient, as it would not explain how the method was applied in the particular case of the use of FRT, including all the processes it involves, and not just the technical one. Furthermore, even if this method is patented, like Clearview AI's, the publication of the patent shows technical experimentation in a controlled environment opposed of environment of practical use.

[225] For example, the FRTs used by the FBI are subject to an annual review by NIST. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Facial Recognition Technology (FRT). Available at: https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0 . Accessed on: February 22, 2024.

[226] The search was carried out on March 10, 2024. The IEEE Xplore exportable database is available at https://ieeexplore.ieee.org/Xplore/home.jsp.

Figure 23. Example of the number of peer-reviewed and published articles on FRT methodology



Source: prepared by the author based on data from IEEE Xplorer.

Rate of Error. The debate around accuracy has been central to stabilizing the credibility of the algorithm. Particularly since 2018, as criticism of FRT has grown, companies have spontaneously submitted their algorithms to NIST accuracy tests. As noted in the previous chapter, Clearview advertises an accuracy rate of 99%, leading to a claim of an “almost perfect” algorithm according to the metrics used by the NIST. However, as analyzed in section 4.3, no single methodology indicates this error rate when algorithms are used in practice. Furthermore, despite the existing statistics of FRT error rates, they fail to inform the potential risks of error resulting from widespread use of such technology, given that output is the materialization of a multitude of human and non-human entanglements. Furthermore, security agencies do not produce data and reports showing the number of searches carried out and the ratio of false positives and negatives of the technology they used. In other words, there is no data production on errors or this technology's "real-world" efficiency (GARVIE, 2022, p.46).

Furthermore, there are no standards or regulations required to control and normalize the use of TRF in the United States and in most countries where these tools are being used in security practices and in the Criminal Justice System. In the specific case of the US, standardization bodies including the Facial Identification

Scientific Working Group[227], the Organization of Scientific Area Commissions[228], the International Standards Organization (ISO)[229] and others are working to develop recommendations. However, there is no reasonable guarantee that they will be followed in the same way as existing "best practices" and recommendations. According to Garvie (2022), reliable principles and methods are only as good as their practical application.

Last step of Daubert methodology of admissibility, General Acceptance. FRT and other machine learning applications have generally gained acceptance within the technical-scientific community, as discussed in chapter 2, as well as gaining relevant adherence in the field of security and legal experts. However, this factor can be complex to quantify. As Garvie (2022) argues, even if we only take the perspective of the scientific-technical community that supports the use of technology, the method still fails in the latter condition. As mentioned earlier, with the proliferation of methods and practices for operating FRTs, none are considered standard, i.e., there is no widely accepted technique within a relevant scientific context.

In addition to these five pillars, courts may consider other factors when assessing admissibility. Therefore, even if the results of FRT are not admissible under the five factors listed in Daubert, courts may still admit those results as evidence. In this case, the defendant has the right to challenge and cross-examine that evidence. However, according to Garvie (2022), precedents could also be set to extend this evidence's credibility and use. As Cole (2005) demonstrates, fingerprints were not initially considered scientific evidence in the terms established by the Daubert method; still, they were given credibility and admitted in court.

[227] The Facial Identification Scientific Working Group (FISWG) develops consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human facial features. FACIAL IDENTIFICATION SCIENTIFIC WORKING GROUP (FISWG). Available at: https://www.fiswg.org/ . Accessed on: February 22, 2024.
[228] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Organization of Scientific Area Committees for Forensic Science. Available at: https://www.nist.gov/organization-scientific-area-committees-forensic-science . Accessed on: February 22, 2024.
[229] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Available at: https://www.iso.org/standard/87734.html . Accessed on: February 22, 2024.

For Jasanoff (2005, p.139), "[u]ncritical reliance on 'good science' in the law is not only problematic from a practical standpoint, it may also be inadequate to do justice." Several researchers express concern about Daubert's practical applicability, even in non-algorithmic evidence (EDMOND, 2012; JASANOFF, 2005; LYNCH, 2008; COLE, 2015). Criticism has mainly gone in three directions: that the criteria in the Daubert case were unclear, that judges would be ill-equipped to evaluate complex scientific methodologies, and that Daubert seems to have made it difficult for the defense to produce expert evidence – overall, there is a hegemony of the expert, of science over the lay public (LYNCH, 2009; COLE, 2015). The increased use of algorithms is not accompanied by procedures to examine innovation or suspects' rights and defendants' rights to deal with errors and human and mechanical biases. Jasanoff (2005, p.45) emphasizes that "judges cannot hand over to scientists their responsibilities as guardians of the evidence, nor can they insist on impossibly high standards of scientific rigor." Here, it becomes clear how the boundary between science and litigation, for example, is significantly blurred in practice and the product of complex socio-technical negotiations.

According to Jasanoff (2005, p.45), Daubert and his "offspring" widened the courts' room for maneuvers concerning the admissibility of scientific-technical evidence. As analyzed in this section, in the US, judicial precedents dealing with the control of the reliability of scientific evidence did not stop with Daubert but went further. In a groundbreaking 2020 decision, the New York State Supreme Court expanded the meaning of the “relevant scientific community”. The case dealt with the reliability of micro ballistic confrontation forensic examinations[230]. The judge in the case, April Newbauer, felt that she should listen to experts from the community of forensic scientists working in micro ballistics and experts in scientific methodology, psychology, and statistics[231]. Needless to say, such position led to a broadened understanding of who is considered an expert to speak with authority about those matters. When machine learning algorithms are added, the models are also classified as experts, as seen in section 5.1.

[230] JUSTIA LAW. 2020 NY Slip Op 20153. Available at: https://law.justia.com/cases/new-york/other-courts/2020/2020-ny-slip-op-20153.html . Accessed on: February 22, 2024

[231] SUPREME COURT OF THE UNITED STATES. Opinion 20-637. Available at: https://www.supremecourt.gov/opinions/21pdf/20-637_10n2.pdf . Accessed on: February 22, 2024.

Knowledge does not mean the end of the reduction of ignorance. "Ignorance is an integral part of accumulating specialized knowledge" (LEANDER; WEAVER, 2018, p.11). The production of knowledge by and through algorithms can generate new forms of ignorance, uncertainty, or ambiguity. Doyle (2018) conducted extensive research on the quality management of forensic science and its relationship to justice. He concluded that the main challenges currently faced in all forensic fields are the premature use of technical and methodological innovations in science and technology that are outside a framework of quality standards, lack of standardization and harmonization, and lack of resources and accountability. Interpol further emphasized these issues as severe challenges in digital evidence (REEDY, 2020) and the UK's National Digital Forensics Strategy[232].

As FRT enters the mainstream of criminal proceedings, there are multiple admissibility challenges for each vendor or model – and possibly for each machine learning algorithm. It is worth noting that the investigation of admissibility through the Daubert norm of evidence is about the reliability of the technique. We should note that even if the algorithmic evidence resulting from algorithmic recognition can be considered 'reliable' under the Daubert methodology, it is not free of errors and flaws. It is, therefore, important to look at how credibility is assembled in different ways and practices. As Jasanoff (2005) and Bal (2005) point out, we should not assume certainties about how scientific-technical evidence can be received in court. Perceptions of the credibility, competence, or relevance of evidence can vary.

One example is the admissibility of DNA as scientific evidence in the courts. DNA came to be associated with adequate and legitimate evidence through evidence acquires meaning within various practices of knowledge production and shared values about what should be accepted as evidence. valid practices considered normatively adequate and legitimate. However, the immutable and powerful "gold standard" image associated with early cases of forensic DNA evidence proved fragile when informed lawyers exposed irregularities and questionable practices

[232] NATIONAL POLICE CHIEFS' COUNCIL (NPCC). National Digital Forensic Science Strategy. Available at: https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf . Accessed on: February 22, 2024.

involved in producing such evidence (LYNCH et al. 2008). Re-establishing the epistemic authority of DNA as evidence involved a combination of bureaucratic and technical interventions to avoid future legal challenges (LYNCH et al. 2008).

Smith (2022) identifies similarities between the process of admissibility of DNA and fingerprint evidence, on one hand, and the debates about evidence anchored in algorithmic results, on the other. According to the author, the paths taken by fingerprint and DNA evidence lead one to believe that FRT will gain acceptance as reliable evidence as bureaucratization and adjudication processes occur, precedents are created. The refinement of admissibility is just one piece of the puzzle in which the algorithm crystallizes its way of telling the truth as good enough to do 'better justice.' According to Jasanoff (2006, p.333), without giving up the principle of truth, scientists, jurists, and policymakers can define legitimacy in the decisions they make as factual enough to appreciate the actions expected of them.

We have seen, this way of thinking and doing can open up epistemological and material horizons for the practices of legal and security professionals. Material-discursive practices are "continuous material (re)configurations of the world" (BARAD, 2003, p.822). The performance of this evidence or their superimposition is a continuous entanglement with the thought and matter of the conditions of the possibility of reality. As a scientific apparatus, the resulting facial recognition system is "a specific engagement of the world where part of the world becomes intelligible to another part of the world" (BARAD, 2007, p.342). If it is true that data has long served as forensic evidence that encapsulates the actual processes of the world (HACKING, 2006; DESROSIÈRES, 1998), intelligibility can also result in excluding alternative narratives and other "ways of telling the truth." In this sense, the expert's figure and the algorithm's framing as an expert are embedded in and a product of what Cole (2001, p.15) has called the historical commitments of science and the law for the production of order.

As legal cases proliferate amid errors and the difficulty of making algorithmic processes intelligible, the demands are for the search for a single identifiable agent, the human in the circuit. However, the analysis clarifies how the first-person account is impossible. Algorithmic systems always involve humans and

technologies, albeit in different ways, and human-technology entanglements are integrated into a chain of decision and command (DE GOEDE, 2018). In this sense, trust in these technologies, in the absence of data on their use and efficiency in practice, as has been the case with the use of facial recognition by security agencies and legal professionals, is, therefore, best understood as a collaborative realization, undertaken in the service of pragmatic and 'useful' ways of acting amid uncertainty. The practice of telling the truth of FRT goes beyond interpretation or the presentation of legal arguments; it allows for an analysis of how stories are interpreted and stitched together as a "true" story about the evidence. As Latour discusses, unlike scientific results that remain contested, the law comes to an "arrêt" after a trial (LATOUR, 2010). Legal discussions end, and their results become standardized legal facts that can serve as precedents for upcoming cases. Moreover, a trial is more than an "arrêt"; it is a judgment of factual or legal truth (VALVERDE, 2009, p. 7-11).

The claim to a foundation of truth in the algorithmic results present in the application of the Criminal Justice System, which has permeated our contemporary political imagination, offers technical-scientific solutions to resolve the difficulties of decision-making amid uncertainty so that order can be ensured. With a view to materialize and maintain order, it is necessary to keep under control what exceeds and disturbs the possibilities of (dis)order. After all, what is at stake, as I have observed in this section, is not only how scientists and developers produce algorithms for legal use but also how algorithmic reason supports ideas of causality, reason, and justice in the law and how algorithms can complement the work of legal professionals in the project of guaranteeing social stability and order. Even amid an entanglement of (dis)ordered and messy practices.

5.4. The indeterminacy: the (im)possibility to encode justice

The indeterminacy of the tangled practices of security and legal professionals with machine learning algorithms leads to many difficult questions about how to disentangle issues of error and "doing justice." At this point in this dissertation, it is worth reinforcing my commitment to "stay with the trouble" (HARAWAY, 2026) to provoke thought about the complexity of the

materialization of FRT as an apparatus for producing evidence with/within and through the criminal justice system, not to solve it.

Thus, despite presenting the errors of FRT in practice through stories and data, it is not the focus of this research to denounce FRT failures. However, I propose reading how these technologies, despite their limitations and inaccuracies, have created conditions of possibility for a way of thinking and carrying out a specific practice of identification and recognition in security practices that is perpetuated and reinforced. As we have analyzed in this thesis, the algorithmic reason is a distinct type of rationality (ARADAU; BLANKE, 2022, p. 3-4), which creates the conditions for the possibility of practices and the production of datified subjects through the promise of a more efficient decision.

This chapter aims to provide a diffractive reading of how FRT evidence stabilizes and assembles trust and epistemic validity. As an apparatus, FRT cuts through how probable cause for identification and suspicion is presented as entangled with the practices of security and legal professionals. This mode of recognition is framed as reliable enough even amid criticism, the messiness of methodologies, and the lack of 'scientific' standards. I emphasize with this analysis that the legal norm itself has been made in practice with and through algorithms. The stabilization and circulation of these socio-material and legal norms and practices allow and normalize error and the differential distribution of (in)security and rights in practice.

Although FRT is framed as an efficient tool for security and optimizing justice, we have seen that it reproduces and produces other forms of violence and injustice (BENJAMIN, 2019; EUBANKS, 2018; O'NEIL, 2017). Assuming that artificial intelligence is a "powerful tool" for optimizing security and justice, according to the report by the Journal of the National Institute of Justice USA (2019) presented in section 5.1, the question is: for whom is it being optimized? Machine learning algorithms are more than just practical tools. They are part of how problems and solutions are framed (AMOORE, 2020) and part of broader power structures and relations (CRAWFORD, 2021). All the cases reported here of errors and failures are of non-white people, which does not mean that white people are not affected by the expansion of surveillance and the use of these technologies,

but that there are groups that are preferential targets. Non-white people are disproportionately enrolled in police databases and are over-represented in the US prison system (WANG, 2016; BENJAMIN, 2019; EUBANKS, 2018; O'NEIL, 2017).

While discriminatory policing is endemic in the US criminal justice system, FRT practices can contribute to reinforcing this way of doing security (FERGUNSON, 2016; BROWNE, 2020; WANG, 2019). As we noted in chapters 2 and 3, in addition to the fact that FRTs are known to have lower accuracy rates with specific demographic groups, there is a history of "shining a light" on black bodies by producing data to control what was perceived as an anomaly (BROWNE, 2020). Since the efforts to establish biometrics as a scientific field, there has been an effort to identify and recognize possible deviations. As described in chapter 3, a colonial legacy of body datification has disproportionately affected specific groups. Rather than a neutral technology, FRT has been a "potent lever of social regulation that serves specific race and class interests" (PAGLEN, 2016, p.10).

In this dissertation, I have emphasized that the historical, political, and social conditions of the emergence, circulation, and stabilization of practices of thinking and doing security are important not only because they support discourses that are generative factors of real actions and modulation of norms but also because security itself materializes through the intra-activity of the world in it becoming (BARAD, 2007).

Likewise, what is framed as error, failure, or optimization also emerges from this intra-activity. Errors are acceptable and understood as side effects in order to optimize the system, and this can be thought of not only in terms of the algorithm but also of the criminal justice system in which it is entangled. Thus, problematizing error and failure by raising questions about how and what should be optimized and which errors should be accepted and/or normalized can help challenge simple solutions. In other words, the circular argument is that the error can only be solved by algorithmic optimization, which is why improving the technique is sufficient for the technical problem.

The examples presented in this chapter of how recognition by algorithms makes speculative security action possible bring to light and make visible the frictions of how the legal norm has been applied in practice and how, by recognizing the error, it may be possible to attempt, at the limit, a reparation based on the recognition of that error. However, some questions still echo: How many cases cannot be classified as errors? How can we recognize what an FRT error is? What can recognize this error create regarding the possibility of action and contestation?

As noted in the section above, investigative evidence used by security agencies has a lower standard and technical-scientific rigor than in court due to the assumption that investigative leads will be confirmed with other evidence before establishing “reasonable suspicion” for arrest. However, we observed in a sample of cases studied in this thesis that the FRT was framed as reliable to provide a basis of probable cause for an arrest. No other evidence seemed to link Randal Reid, who lives in Georgia, to the robberies in Louisiana, a state he never visited. No Detroit police investigator obtained location data from Robert Williams' phone to see if he was in the store on the day, he carried out a robbery. The police consulted a security contractor, who analyzed surveillance video of the robbery incident and then selected Williams from a list of photos of six people. However, the security contractor was not in the store when the incident occurred and never saw Williams in person.

We observe how the legal norm materializes through a flaw in due process, which is the right to a fair trial in practice. This failure or 'adaptation' reinforced in practice the comprehensive understanding of the reliability of FRT used in criminal investigations despite the lack of comprehensive understanding of how FRT works. When coupled with our algorithmic results, this assertion about the confidentiality of a previously unknown suspect in the cases analyzed affects how a specific law enforcement officer matches and how much additional evidence must be collected before probable cause is established. As I pointed out, the line between using algorithm results as clues or as evidence of probable cause for punitive measures is blurred. Moreover, without data on how FRTs are used in practice, we have no idea how well they are an investigative tool, how strong the evidence is, and how often people are wrongly identified.

Furthermore, despite the central role that facial recognition has played in the stories told in this chapter, security agencies do not consider themselves obliged to divulge details about the uses of these technologies to the people affected by them or who have encountered the criminal justice system through them. Thus, the fact that facial recognition has not been introduced as evidence in court through the attribution of scientific validity, such as Daubert, does not mean that it has not been used as truth-telling evidence against someone – a reliable way of telling the truth about a suspect's identity. It also means that an unknown number of approaches, cases of arrests, and subjects have not had the opportunity to challenge the main evidence linking them to a crime. The security practice of algorithms provides material, legal, and political support for specific forms of (in)security.

The debates around errors, as we have seen in this dissertation, have defined that there should be a standard and regulation on the use of FRT, the search for more accurate technologies, and the reaffirmation of the human in the loop as the locus of legitimacy of the results, with the creation of protocols and training, on the one hand (JOHNSON, 2023; GARVIE, 2022). On the other hand, pressure has been growing for accountability for mistakes (as in the civil litigation cases mentioned in section 5.2) and for limited use or ban movements (HILL, 2023). Precedents and policies have also been established through civil litigation processes to limit the use and produce disruptions in the constant flow in which algorithmic reason circulates. These tensions and controversies help to foster a legal, regulatory, and political debate.

As Hildebrandt (2014) suggests, it is crucial to consider the material conditions of possibility for legal regulation. It is essential to remember that transparency standards and accountability frameworks are not always readily available for challenge (ANNANY, 2020). Rather than erasing politics in algorithmic processes (ARADAU; BLANKE, 2015), other forms of political contestation that can be just as complex often emerge (MONSEES, 2019).

Algorithmic reason allows for the diffusion and decentralization of practices (HUYSMANS, 2014; ARADAU; BLANKE, 2022; AMOORE, 2013; 2020). The "problem of many hands" (NISSENBAUM, 1996) is the multitude that emerges from the dispersed and heterogeneous tangle of practices with the algorithm that makes it difficult to challenge and contest the results. When violence or harm is recorded, there is a vocalization of guilt; one thinks of a unified entity whose choice and agency can be held accountable, as we observed in the cases presented. Identifying a single source code or place of authorship complicates consistent attempts to hold algorithms accountable. Traditional notions of human autonomy and responsibility do not apply to algorithmic entanglements.

These observations are not meant to detract from the importance of attempts to regulate practices with algorithms. Nevertheless, I am drawing attention to how debates about algorithmic error and failure can be a productive methodology if we do not just look at it as a point that can be improved. It is because showing and telling about the error can invert the typical assumption that the constant search for better precision, explainability, and 'ethics by design' should lead to greater objectivity, efficiency, and accountability in using algorithms to solve complex social issues in the criminal justice system. The problem is not just technical but composed of a network of heterogeneous practices that circulate so that there are conditions of (im)possibility for codifying justice through algorithmic optimization alone.

The invitation is to think about the conditions of possibility beyond technical-scientific solutions. The forms of contestation and critique of FRT in the justice system are complex. It is, therefore, necessary, as we argued in chapter 2, not to appeal only to the search for foundations or origins of "opening the black box" or to the legal domain alone but to think of algorithms as political and to make political claims that are not yet recognized in the existing terrain of rights. Our ability to resist and contest also depends on destabilizing worldviews, on reimagining possibilities for creation and invention – the lines of ascent, which Deleuze and Guattari (1987, p.276) called lines of flight – the risky movement outside the already known, the dreamlike space where the improbable can be imagined. A space of creation that takes us out of predictable repetitions and into unexpected situations. Lines of ascent and descent are not a choice of either/or, but

always, and they function in "a dynamic game of (in)determination" (BARAD, 2015, p. 160).

Instead of proposing certainties and solutions, I propose leaving the door ajar. As Amoore (2020) argues, indeterminacy reopens algorithmic multiplicity, where the hinge does not completely demarcate the axis of possible movement. The claim for a foundation of truth in data that permeates our political imagination has closed the door to other futures, offering algorithmic solutions to close the gap and solve the difficulties of decision-making and "doing justice." In this sense, re-establishing doubt within the algorithm and allowing the formed components of the composite to understand and talk about its limits is seeking to leave the door ajar to make other political claims (AMOORE, 2019; 2020; CRAWFORD, 2021). As Benjamin invites us in "Imagination: A Manifesto" (2024), we must take imagination seriously as a powerful tool for political contestation and a means of challenging the modes of oppression that structure our society.

Finally, without losing sight of what algorithmic reason makes possible in the practices of security and legal professionals and how they materialize and legitimize discriminatory and violent actions in different contexts of experimentation, we are invited to maintain the speculative commitment to think about how things might be different (PUIG DE LA BELLACASA, 2017, p.17) or not. To keep the cracks in material-discursive practices visible. In this context, rethinking error could be a possible way of understanding the complexity of the ambivalent implications and consequences of the material-discursive practices of algorithmic reason in security practices.

6.
Taking the entanglements of algorithms and security and legal professionals seriously

If a machine is expected to be infallible, it cannot be intelligent either.

Allan Turing, 1947.

Technology is not the design of physical things. It is the design of practices and possibilities.

Lucy Suchman, 2007.

In this dissertation, I explored how entanglements of (in)security are configured, adjusted, reshaped, stabilized, and disseminated through the practices of security and legal professionals with and through machine learning algorithms. To this end, I carried out a diffractive reading composed of and in conversation with different fields to understand how the trust of the algorithm as an apparatus, its epistemic authority, is assembled, even when they are publicly understood to be flawed, prone to errors and biases.

Rather than emphasizing the opacity, impartiality, and need for error correction of machine learning algorithms, I suggested we pay attention to the multiple material-discursive practices that take place among a multitude of dispersed actors that enable the operation of algorithmic reason as a knowledge apparatus good enough to anchor the actions of security and legal professionals. The dispersion of algorithms in security practices means that they come to shape ingrained habits and dispositions. They become what Bourdieu (1990, p. 53) described as "structuring structures". And through delving into Clearview AI and error stories, I observed how algorithmic reason sustains practices and destabilizes distinctions of what is an error, what works and what does not.

As a particular material-discursive set, machine learning algorithms "doing" and "think" in a way that can also change the way we think about the world as they "redistribute" the sensible (RANCIÈRE, 2006). The materialization of algorithmic entanglements and their meaning is conceived as an integrated whole, interweaving the material, the semiotic, the scientific, and the imaginary (SUCHMAN, 2007). As

analyzed in chapter 3 of this research, the very condition of possibility for the development of FRT is entangled with power asymmetries and political-social structures that reproduce a way of ordering and organizing societies (BENJAMIN, 2019; BROWNIE, 2010; CHUN, 2021; CRAWFORD).

In Part I of this thesis, I analyzed how algorithmic systems are seen as powerful allies by those who aim to tame an emerging world into a seemingly rational and, therefore, more predictable reality (ROUVROY, 2013,146-147), often with claims of their unparalleled precision operating in a mode of cognition beyond the human capable of analyzing growing masses of heterogeneous data. The algorithm seems efficient and practical in ordering data, people, experiences, and complex temporalities as frictionless narratives for action in the present. The promise of artificial intelligence and machine reading algorithms offers technical and efficient solutions to complex socio-political problems.

Algorithmic representations are not merely reducible to discursive analogies or elements derived from the imagination of experts or users. They are organizational in that they establish a process of continuous changes in the relationships between elements in socio-material configurations, attributing meaning to each element and the entanglement as a whole. As we noted in part II of this thesis, security, and legal professionals understand and apply FRT according to their practical practicality, and this practice, in turn, shapes optimizations and adaptations of the algorithm in search of a configuration that works.

As digital technologies and algorithmic rationalities increasingly reconfigure themselves as security practices, critical scholars have drawn attention to their performative effects on the temporality of law, notions of rights, and understandings of subjectivities (ROUVROY, 2015; AMOORE, 2013; DE GOEDE, 2018). These performative effects can imply uneven distributions of (in)security when cutting and considering what matters based on a data set. In chapter 2, we noted how algorithms should be understood as much more than just security tools. They intra-actively participate in what we think and understand as a security problem and solution: who needs to be protected and who is the target. In this research, I understand algorithms as knowledge devices that function in how we perceive and understand our security issues; they generate performative effects in the production and reconfiguration of realities and characteristics. Indeed, this

question of how machine learning algorithms operate directs attention to their ontoepistemological foundations, as to what emerges from this analysis.

An important point for this dissertation was how machine learning algorithms create possibilities for specific forms of perception, recognition, and identification, and that is why we focus on FRT research. The question of how we discuss recognition is central to access to rights and political participation. It is also central to the way security practices operate through the recognition of anomalies. Machine learning algorithms are enabling practice models that redefine the boundaries of who or what can be recognized. What is at stake is not just who or what is recognized but how the recognition regime generates claims, as judged by the algorithm, and what this makes possible in terms of security actions and violation of fundament rights.

What is being materialized through algorithmic reason is a guideline to "tell the truth" about someone that frames how decisions can be made without room for doubt with biometric data. Algorithms "tell" a true narrative despite being probabilistic and within an experimental epistemology (error is a possibility for improvement and accuracy of the algorithm). Moreover, it analyzes how the adaptive threshold (the power of arrangement and rearrangement of modulations) recursively traces the limit of a possibility and generates a capacity for recognition and perception of a subject and/or a reality.

The algorithm's way of truth-telling helps organize and frame the world, making it intelligible and, in a certain way, "ordered." Truth becomes less a factual representation of a consensual reality and more often an amalgamation of fragments of available data (CRAWFORD, 2021, p.96). As demonstrated by Amoore (2013, p.66; 2020), algorithmic security does not operate based on pre-defined norms but with what she calls a "mobile norm" – a norm that is itself modulated and random, governed not by standards of normality and deviation, but by differential curves of normality. The epistemological coding of algorithmic reason is not based on the dichotomy between truth and falsehood but on the effectiveness of a specific algorithmic set.

In short, the world of algorithms is flat in a non-pejorative sense (INTRONA, 2017). Algorithms have no idea of the world outside of data, symbols,

and meaning, or thought and imagination, and the context in which they learn and operate (BOYD; CRAWFORD, 2012; AMOORE. 2020; CRAWFORD, 2021). Therefore, I focus on how algorithms are displacing questions of error and truth. Instead of resolving questions of error, algorithms develop and learn to operate through their normalization.

I opened this chapter with a quote from Alan Turing in his talk to the London Mathematical Society (1947), where he first disclosed his ideas about a digital computer: he elaborated on the conditions under which a machine would be considered intelligent. Turing recognized that the perfect and continuous processing of information is opposed to any conception of intelligence in computing. He pointed to failure, or even error, as a necessary part of learning and cultivating intelligence in machines. For one of the pioneers in AI, it was a departure not only from the expectation that the machine would perform perfect calculations but also from the machine's calculation process itself. In machine learning algorithms, the process is uninterrupted in that its error does not appear as a break but as part of learning. Errors are not bugs or side effects solved by optimizing the machine learning algorithm but are part of the materialization of material-discursive practices that the algorithm has made possible.

The error does not limit the use of FRT and its circulation and use from policing practices to the courts. However, it helps to proliferate the broader digitalization of domains of everyday life, demanding the expansion of available data to improve the algorithms' accuracy. We can observe that there is a circular pattern of problematization. If the facial recognition algorithm (optimized solution) makes a mistake, this error is part of optimizing the algorithm and improving its accuracy. In this sense, the error is not a problem but part of the solution for which the algorithm offers an "optimized" version – a necessary step towards eventual 'success' (LESLIE, 2018).

There is a body of debate about the errors, opacity, impartiality, and the very limits of the use of FRT in the criminal justice system. Among the controversies are also the peculiar forms of knowledge, advantage and ignorance that these systems generate (INTRONA, 2016), their ethical problems (HU, 2018; AMOORE, 2020; CRAWFORD, 2021), their political consequences (AMOORE, 2020; EUBANKS, 2018), and their feedback on the formation of "targets" that they should read simply

(AMOORE; RALEY, 2017). In this context of the emergence and rise of an algorithmic reason as an apparatus for knowledge of security practices, what matters is not primarily the identification and regulation of algorithmic errors but, more significantly, how algorithms are implicated in new verification regimes (AMOORE, 2020; ARADAU; BLANKE, 2022).

As analyzed, the problematization, discursive circulation, and political responses to FRT problems were shaped by ambiguous figures such as the "black box" or the "biased algorithm." In a context where the materiality and agency of algorithms are heterogeneous, figures that fix complex and multiple sets in a single entity simplify the debate and reinforce a public perception of the (im)possibility of understanding algorithmic practices and, therefore, of 'doing justice.' (JASANOFF, 2005). However, before being black box engines of computational orders, FRTs are everyday practices of different human and non-human actors circulating in dispersed spaces. As I noted in Part II, ultimately, what must be negotiated and governed is not just a technological object but a set of protocols and procedures comprising organizational habits, legal rules, analog artifacts, and technological knowledge.

Law and science, intertwined, endorse a traditional and respected method to guarantee the validity of decisions made by the state (JASANOFF, 2005; COLE, 2015). As institutions for the production of order, the intra-activity between legal and technical-scientific practices creates the conditions for the materialization of a broader way of seeing the proper functioning of society. When flawed and ambiguous guidelines and processes govern their interactions, the ability of any of these spheres to restrict arbitrariness is significantly diminished (JASANOFF, 2005, p.56). Therefore, contestability, making the algorithmic mode of truth-telling in the materialization of evidence open to scrutiny and disagreement, is a challenge that also, in the case of algorithmic rationality, can be productive for "re-imagining and re-politicizing failure." (LISLE, 2017, p.2-4) and open up to a multiplicity of other possible modes of action and political imagination (AMOORE, 2020; CRAWFORD, 2021; ARADAU; BLANKE, 2022).

The re-imagining of error offers a capacity for disruption and surprise, as well as unpacking accepted and crystallized ways of thinking and doing security. The re-politicization of error involves making FRT's tangled, experimental,

dynamic, and ambivalent nature perceptible. At the same time, it is not to limit criticism to their demonstration with the presumption of correcting them but to 'stay with the trouble' (HARAWAY, 2016). Exposing algorithmic bias and its composition can contribute to friction in the dynamic flow that makes the error tolerable by looking at its potential technological optimization. The error may be a mechanism for contesting the cuts, closures, exclusions, and violence that are instantiated as the FRT (as an apparatus) instantiates a particular form of perception, recognition, and identification of anomalies. This cutoff is not finite but rather a dynamic representation of a limit that configures who can be recognized in a particular way with significant material impacts.

As I proposed in Chapter 5, accepting Amoore's (2020, p.152) challenge, we should understand the algorithm not as something that closes the door but as a "hinge" in which the idea of policy itself can change, as something that does not limit future movements. It operates on the margin of doubt (AMOORE, 2019), and doubt itself can be an opening to multiplicity. Furthermore, analyzing the tangle of FRT practices leads us to reflect on the relationships between (dis)united human and non-human actors and digital and analog objects that materialize actions through and from these experimental entanglements. Indeterminacy points to a potential for both ordering and disorder. Each materialization process is permeated by an infinite set of impossibilities of materially reconfiguring present, past, and future worlds; "certainly these questions are nothing less than questions of justice" (BARAD, 2020, p.92).

In this dissertation, I have been careful with the debate about justice. Unlike law, which is instrumental in norms, interpretations, and calculations, "justice is the experience of the incalculable, of having to calculate with the incalculable" (SINNERBRINK, 2006, p.489). As seen in the examples of the stories told in chapter 5, what is at stake in the singular moments when we cannot determine the fair outcome or decision in a given situation, not only because there is no determined norm to be applied, but because the norms, on their basis, are in question and being made more flexible in practice. Norms are being instantiated through FRT from the practices of security professionals to the courtroom.

The tendency is for us to become comfortable with our frames of reference. However, unpacking the imaginaries of what algorithms are and can do in the

criminal justice system can help us understand how these technologies can stifle possibilities for action and legitimize violent and exclusionary practices in an attempt to stabilize order and tame uncertainty. What is being avoided is not the danger of the known subject but the danger of not knowing how to identify and recognize this likely subject (PUAR, 2007, p.185). In this sense, this rationality touches on a point widely shared among diverse efforts to manage risky futures within and beyond security.

As Derrida emphasizes in "Force of the Law" (2007), justice is always to come. Moreover, this quest to imagine a fair way to come paves the way for ethical practice (BARAD, 2020). It is where the infinite possibilities of (re)imagining and perhaps creating conditions for the emergence of a reality in which forms of violence and historical systems of oppression can be eliminated. It seems naive, but as Benjamin (2024) reminds us, the ability to dream can be a possible collective tactic to produce friction in the dominant imaginaries of which worlds are possible. Ultimately, I propose a more modest, indeterminate, and open-ended endeavor where what counts as "better" is always a matter of our concern in the process of "thinking carefully" (PUIG DE LA BELLACASA, 2017, p.59) in addition to a "speculative economy of the promise" of science and technology (STENGERS, 2023, p.88).

Indeterminacy and the possibility of (re)imagining do not prevent us from stepping back from observing and exposing the cracks and ambivalences of the entanglements of (in)security that machine learning algorithms make possible. It also allows us "respone-abibility" (BARAD, 2007; HARAWAY, 2016). We can think of this ability to respond collectively and relationally as a way of responding together and taking seriously the entanglement of algorithms, data, security, and legal professionals that materialize as good enough security practice.

References

9 WAYS TO SEE A DATASET: What's at stake in examining datasets? Available at: https://knowingmachines.org/publications/9-ways-to-see/essays/9-ways-to-see-a-dataset. Accessed on: December 26, 2023.

A POLICY FRAMEWORK FOR RESPONSIBLE LIMITS ON FACIAL RECOGNITION USE CASE: Law Enforcement Investigations (Revised 2022). Disponível em: https://www.weforum.org/publications/a-policy-framework-for-responsible-limits-on-facial-recognition-use-case-law-enforcement-investigations-revised-2022/. Acesso em: 5 jan. 2024.

AAS, K. F. "The body does not lie": Identity risk and trust in technoculture. Crime Media Culture, v. 2, n. 2, p. 143-158, 2006.

AAS, K. F. From narrative to database: Technological change and penal culture. Punishment & Society, v. 6, n. 4, p. 379-393, 2004.

ABDI, HERVÉ; WILLIAMS, LYNNE J. Principal component analysis. Wiley interdisciplinary reviews: computational statistics, v. 2, n. 4, p. 433-459, 2010.

ABEBA, BIRHANE. The unseen Black faces of AI algorithms. Nature, v. 610, n. 7932, p. 451-452, 19 out. 2022.

AI INSIGHT FORUM - Statement from Hoan Ton-That CEO Clearview AI - November 1st 2023. Disponível em: https://www.clearview.ai/ai-insight-forum . Acesso em: 7 nov. 2023.

AL-ALLAF, OMAIMA N. A. Review of face detection systems based artificial neural networks algorithms. arXiv preprint arXiv:1404.1292, 2014.

AMELUNG, N.; GRANJA, R.; MACHADO, H. "We are victims of our own success": Challenges of communicating DNA evidence to "enthusiastic". In: DAVIES, S. R.; FELT, U. (Eds.) Exploring science communication: A science and technology studies approach. London: Sage, 2019.

AMOORE, L. Data Derivatives. Theory Culture and Society, v. 28, n. 6, p. 24–43, 2011.

AMOORE, L. The Politics of Possibility. Duke University Press, Durham, 2013.

AMOORE, L.; PIOTUKH, V. Introduction. In: AMOORE, L.; PIOTUKH, V. (eds) Algorithmic Life, p. 1–18. Routledge, London, 2016.

AMOORE, L.; RALEY, R. Securing with Algorithms. Security Dialogue, v. 48, n. 1, p. 3–10, 2017.

AMOORE, L. Algorithmic war: Everyday geographies of the War on Terror. Antipode, v. 41, n. 1, p. 49-69, 2009.

AMOORE, L. Cloud Ethics: Algorithms and the Attributes of Ourselves and Others. Duke University Press, 2020.

AMOORE, L. Machine learning meaning making: On reading computer science texts - Louise Amoore, Alexander Campolo, Benjamin Jacobsen, Ludovico Rella, 2023. Disponível em: https://journals.sagepub.com/doi/full/10.1177/20539517231166887. Acesso em: 10 set. 2023.

AMOORE, L. Security and the claim to privacy. International Political Sociology, v. 8, n. 1, p. 108-112, 2014.

AMOORE, LOUISE; PIOTUKH, VOLHA. Life beyond big data: Governing with little analytics. Economy and Society, v. 44, n. 3, p. 341-366, 2015.

AMOORE, LOUISE. Cloud geographies: Computing data sovereignty. Progress in Human Geography, v. 42, n. 1, p. 4-24, 2018.

AMOORE, LOUISE. Doubt and the algorithm: On the partial accounts of machine learning. Theory Culture & Society, v. 36, n. 6, p. 147-169, 2019.

AMOORE, LOUISE; HALL, ALEXANDRA. Taking people apart: Digitised dissection and the body at the border. Environment and Planning D: Society and Space, v. 27, n. 3, p. 444-464, 2009.

ANANNY, MIKE. Toward an ethics of algorithms: Convening observation probability and timeliness. Science Technology & Human Values, v. 41, n. 1, p. 93-117, 2016.

ANDERSON, CHRIS. The end of theory: The data deluge makes the scientific method obsolete. Wired magazine, v. 16, n. 7, p. 16-07, 2008.

ANWAR, TASNIM. Unfolding the past proving the present: social media evidence in terrorism finance court cases. International Political Sociology, v. 14, n. 4, p. 382-398, 2020.

ANWAR, TASNIM; DE GOEDE, MARIEKE. From contestation to conviction: terrorism expertise before the courts. Journal of Law and Society, 2021.

APPRICH, C.; CRAMER, F.; HUI, KYONG CHUN, W.; STEYERL, H. Pattern discrimination, p. 124. meson press, 2018.

ARADAU, C. Security that Matters. Security Dialogue, v. 41, n. 5, p. 491-514, 2010.

ARADAU, C.; BLANKE, T. Governing Others: Anomaly and the Algorithmic Subject of Security. European Journal of International Security, v. 3, n. 1, p. 1-21, 2018.

ARADAU, C.; VAN MUNSTER, R. Governing terrorism through risk: Taking precautions (un)knowing the future. European journal of international relations, v. 13, n. 1, p. 89-115, 2007.

ARADAU, CLAUDIA et al. (Ed.). Critical security methods: New frameworks for analysis. Routledge, 2014.

ARADAU, CLAUDIA; BLANKE, TOBIAS. Algorithmic Surveillance and the Political Life of Error. Journal for the History of Knowledge, v. 2, n. 1, p. 10, 2021.

ARADAU, CLAUDIA. Assembling (non)knowledge: Security law and surveillance in a digital world. International Political Sociology, v. 11, n. 4, p. 327-342, 2017.

ARADAU, CLAUDIA. The signature of security: Big data anticipation surveillance. Radical philosophy, v. 191, p. 21-28, 2015.

ARADAU, CLAUDIA; BLANKE, TOBIAS. Politics of prediction: Security and the time/space of governmentality in the age of big data. European Journal of Social Theory, v. 20, n. 3, p. 373-391, 2017.

ARADAU, CLAUDIA; BLANKE, TOBIAS. The (Big) Data-security assemblage: Knowledge and critique. Big Data & Society, v. 2, n. 2, p. 2053951715609066, 2015.

ARADAU, Claudia; BLANKE, Tobias. Algorithmic Surveillance and the Political Life of Error. Journal for the History of Knowledge, v. 2, n. 1, p. 10-10, 2021.

ARADAU, Claudia; BLANKE, Tobias. Algorithmic reason: The new government of self and other. Oxford University Press, 2022.

ARONSON, JAY D. Creating the Network and the Actors: The FBI's Role in the Standardization of Forensic DNA Profiling. BioSocieties, v. 3, n. 2, p. 195-215, 2008.

AUSTIN, J. L. A Parasitic Critique for International Relations. International Political Sociology, v. 13, n. 2, p. 215-231, 2019.

ÁVILA, FERNANDO; HANNA-MOFFAT, KELLY; MAURUTTO, PAULA. The seductiveness of fairness: Is machine learning the answer?–Algorithmic fairness in criminal justice systems. In: The Algorithmic Society. Routledge, p. 87-103, 2020.

BALLANTYNE, JACK; HANSON, ERIN K.; PERLIN, MARK W. DNA mixture genotyping by probabilistic computer interpretation of binomially-sampled laser captured cell populations: combining quantitative data for greater identification information. Science & Justice, v. 53, n. 2, p. 103-114, 2013.

BARAD, KAREN. Getting Real: Technoscientific Practices and the Materialization of Reality. differences: A Journal of Feminist Cultural Studies, v. 10, p. 88-128, 1998.

BARAD, KAREN. Posthumanist Performativity: Toward an understanding of how matter comes to matter. Signs: Journal of Women in Culture and Society, v. 28, p. 801-831, 2003.

BARAD, KAREN. Meeting the universe halfway. In: Meeting the universe halfway. Duke University Press, 2007.

BARAD, KAREN. Erasers and erasures: Pinch's unfortunate 'uncertainty principle'. Social Studies of Science, v. 41, n. 3, p. 443-454, 2011.

BARAD, KAREN. Matter (') s (of) unconscious (ing): Re-membering/reconfiguring () the logics/structure of supplementarity. Dialogues in Human Geography, p. 20438206241240204, 2024.

BARAD, Karen. After the end of the world: Entangled nuclear colonialisms, matters of force, and the material force of justice. Estetyka i Krytyka, v. 58, n. 3, p. 85-113, 2020.

BAUMAN, Z.; BIGO, D.; ESTEVES, P.; GUILD, E.; JABRI, V.; LYON, D.; WALKER, R. B. J. Após Snowden: repensando o impacto da vigilância. Revista Eco-Pós, v. 18, n. 2, p. 8-35, 2015.

BELLANOVA, R.; DE GOEDE, M. The algorithmic regulation of security: An infrastructural perspective. Regulation & Governance, 2020.

BELLANOVA, Rocco; JACOBSEN, Katja Lindskov; MONSEES, Linda. Taking the trouble: Science, technology and security studies. Critical Studies on Security, v. 8, n. 2, p. 87-100, 2020.

BELLANOVA, Rocco et al. Toward a critique of algorithmic violence. International Political Sociology, v. 15, n. 1, p. 121-150, 2021.

BENEDICT, T. The Computer Got It Wrong: Facial Recognition Technology and The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest. 2023.

BENJAMIN, RUHA. Race after technology: Abolitionist tools for the new jim code. Social forces, 2019.

BENJAMIN, Ruha. Imagination: A Manifesto (A Norton Short). WW Norton & Company, 2024.

BENJAMIN, Ruha. Assessing risk, automating racism. Science, v. 366, n. 6464, p. 421-422, 2019.

BERTRAND, RUSSELL. Human Knowledge Its Scope and Limits. New York: Simon and Schuster, 1948.

BEST, J.; WALTERS, W. “Actor-Network Theory” and International Relationality: Lost (and Found) in Translation: Introduction. International Political Sociology, v. 7, n. 3, p. 332-334, 2013.

BEYOND FACE VALUE: Public attitudes to facial recognition technology. Disponível em: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/. Acesso em: 11 mar. 2024.

BIASES IN AI SYSTEMS: A survey for practitioners: Queue, v. 19, n. 2. Disponível em: https://dl.acm.org/doi/10.1145/3466132.3466134 . Acesso em: 26 dez. 2023.

BIGO, D. Beyond National Security the Emergence of a Digital Reason of State(s) Led by Transnational Guilds of Sensitive Information: The Case of the Five Eyes Plus Network. In: WAGNER, B.; KETTEMANN, M. C.; VIETH, K. (eds). Research Handbook on Human Rights and Digital Technology, p. 33-52. Edward Elgar, Cheltenham, 2019.

BIGODE, D.; TSOUKALA, A. (Ed.). Terror insecurity and liberty: Illiberal practices of liberal regimes after 9/11. Routledge, 2008.

BIGO, DIDIER. Security exception ban and surveillance. In: Theorizing surveillance. Willan, p. 60-82, 2006.

BIGO, DIDIER; ISIN, ENGIN; RUPERT, EVELYN (Ed.). Data Politics: Worlds Subjects Rights. Routledge, 2019.

BLAISE, AGÜERA Y ARCAS; MITCHELL, MARGARET; TODOROV, ALEXANDER. Physiognomy's New Clothes. Medium, maio 6, 2017. Disponível em: https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a. Acesso em: 10 nov. 2021.

BOGLE, A. Australian federal police officers trialled controversial facial recognition tool Clearview AI. Australian Broadcasting Corporation News, 2020. Disponível em: https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federalpolice/12146894 . Acesso em: 18 jan. 2020.

BONELLI, L.; RAGAZZI, F. Low-tech security: Files notes and memos as technologies of anticipation. Security Dialogue, v. 45, n. 5, p. 476-493, 2014.

BOSMA, E. Multi-sited Ethnography of Digital Security Technologies. In: DE GOEDE, M.; BOSMA, E.; PALLISTER-WILKINS, P. (Eds.). Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork, p. 193-212. Routledge, London, 2020.

BOWKER, GEOFFREY; STAR, SUSAN LEIGH. Sorting things out. Classification and its consequences, 1999.

BOYD, D.; CRAWFORD, K. Critical questions for Big Data. Information Communication & Society, v. 15, n. 5, p. 662-679, 2012.

BRAYNE, SARAH. Big data surveillance: The case of policing. American sociological review, v. 82, n. 5, p. 977-1008, 2017.

BRAYNE, SARAH; CHRISTIN, ANGÈLE. Technologies of crime prediction: The reception of algorithms in policing and criminal courts. Social problems, v. 68, n. 3, p. 608-624, 2021.

BRECKENRIDGE, KEITH. Biometric State: The Global Politics of Identification and Surveillance in South Africa 1850 to the Present. Cambridge UK: Cambridge University Press, 2014.

BRICE, S. Privacy Implications of Facial Recognition. Medium. Disponível em: https://samdbrice.medium.com/2dbde4de231 a. Acesso em: 11 nov. 2023.

BROWNE, SIMONE. Digital epidermalization: Race identity and biometrics. Critical Sociology, v. 36, n. 1, p. 131-150, 2010.

BROWNE, SIMONE. Dark matters. Duke University Press, 2015.

BROWNE, SIMONE. Race and Surveillance. In: Routledge Handbook of Surveillance Studies. Routledge, p. 72-80, 2012.

BUOLAMWINI, JOY; GEBRU, TIMNIT. Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on fairness accountability and transparency. PMLR, 2018.

BURT, C. Clearview facial recognition added to US federal procurement marketplace. Disponível em: https://www.biometricupdate.com/202403/clearview-facial-recognition-added-to-us-federal-procurement-marketplace . Acesso em: 22 mar. 2024.

CALHOUN, L. Latency uncertainty contagion: Epistemologies of risk-as-reform in crime forecasting software. Dialogues in Human Geography, 2023. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/02637758231197012. Acesso em: 29 dez. 2023.

CAMPBELL, Z. Sci-fi surveillance: Europe's secretive push into biometric technology. The Guardian, 2020. Disponível em: https://www.theguardian.com/world/2020/dec/10/sci-fi-surveillance-europes-secretive-push-into-biometric-technology. Acesso em: 17 set. 2023.

CAMPOLO, ALEXANDER; CRAWFORD, KATE. Enchanted determinism: Power without responsibility in artificial intelligence. Engaging Science Technology and Society, v. 6, p. 1-19, 2020.

CASTRO, D. Survey: Few Americans Want Government to Limit Use of Facial Recognition Technology Particularly for Public Safety or Airport Screening. Disponível em: https://datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-

use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/. Acesso em: 11 mar. 2024.

CELLARD, Lopup. **Algorithms as figures: Towards a post-digital ethnography of algorithmic contexts - Loup Cellard, 2022**. Disponível em: <https://journals.sagepub.com/eprint/ITYRJF2JETRIPPIDBVEG/full#bibr30-14614448221079032>. Acesso em: 10 set. 2023.

CHAMPOD, C.; TISTARELLI, M. Biometric technologies for forensic science and policing: State of the art. Handbook of Biometrics for Forensic Science, p. 1-15, 2017.

CHAN, J.; MOSES, L. B. Is Big Data challenging criminology? Theoretical Criminology, v. 20, n. 1, p. 21-39, 2015.

CHENEY-LIPOLD, JERRY. A new algorithmic identity: soft biopolitics and the modulation of control. Theory culture & society, v. 28, n. 6, p. 164-181, 2011.

CHIN-ROTHMANN, C.; NICOL TURNER LEE. Police surveillance and facial recognition: Why data privacy is imperative for communities of color. Disponível em: https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ . Acesso em: 29 dez. 2023.

CHUN, WENDY. Discriminating Data: Correlation Neighborhoods and the New Politics of Recognition. MIT Press, 2021. E-book.

CHUN, WENDY. Updating to remain the same: habitual new media. Cambridge MA: MIT Press, 2016.

CINO, J. G.; et al. THE ORACLE TESTIFIES: FACIAL RECOGNITION TECHNOLOGY AS EVIDENCE IN CRIMINAL COURTROOMS. University of Louisville Law Review, v. 61, n. 1, p. 137, set. 2022.

CLAUSER, BRIAN E. The life and labors of Francis Galton: a review of four recent books about the father of behavioral statistics. Journal of Educational and Behavioral Statistics, v. 32, n. 4, p. 440, 2007.

CLAYTON, J. Clearview AI used nearly 1m times by US police it tells the BBC. Disponível em: https://www.bbc.com/news/technology-65057011. Acesso em: 30 ago. 2023.

COLE, S. How much justice can technology afford? The impact of DNA technology on equal criminal justice. Science and Public Policy, v. 34, n. 2, p. 95-107, 2007.

COLE, S. Forensics without uniqueness conclusions without individualization: The new epistemology of forensic identification. Law Probability and Risk, v. 8, n. 3, p. 1-23, 2009.

COLE, SIMON A. Suspect identities: A history of fingerprinting and criminal identification. Harvard University Press, 2001.

COLEMAN, LARA M.; ROSENOW, DOERTHE. Security (studies) and the limits of critique: Why we should think through struggle. Critical Studies on Security, v. 4, n. 2, p. 202-220, 2016.

CONGRESSIONAL AND LEGISLATIVE AFFAIRS | NIST. Disponível em: https://www.nist.gov/congressional-and-legislative-affairs . Acesso em: 19 out. 2023.

CORMEN, THOMAS H.; LEISERSON, CHARLES E.; RIVEST, RONALD L.; STEIN, CLIFFORD. Introduction to Algorithms. 3rd ed. Cambridge MA: MIT Press, 2009.

CRAWFORD, K.; GILLESPIE, T. What is a flag for? Social media reporting tools and the vocabulary of complaint. New Media & Society, v. 18, n. 3, p. 410-428, 2016.

CRAWFORD, Kate. Artificial intelligence's white guy problem. The New York Times, v. 25, n. 06, p. 5, 2016.

CRAWFORD, Kate. The atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press, 2021.
CRAWFORD, Kate; PAGLEN, Trevor. Excavating AI: The politics of images in machine learning training sets. Ai & Society, v. 36, n. 4, p. 1105-1116, 2021.

CROZIER, ELISABETH. The Effect of Eyewitness Misidentification on the Criminal Justice System: Procedure Changes and Mitigative Actions, 2023.

CUDWORTH, ERIKA; HOBDEN, STEPHEN; KAVALSKI, EMILIAN (Ed.). Posthuman dialogues in international relations. Routledge, 2017.

DANIEL CHÁVEZ HERAS; BLANKE, T. On machine vision and photographic imagination. AI & Society, v. 36, n. 4, p. 1153-1165, 17 nov. 2020.

DANIEL VASQUEZ E. The New York City Council Committees on Technology and Civil & Human Rights Oversight Hearing on the Use of Biometric Identification Systems in New York City. [s.l: s.n.]. Disponível em: https://bds.org/assets/images/BDS_BiometricTechHrg.pdf . Acesso em: 3 jan. 2024.

DASTON, LORRAINE; GALISON, PETER. Objectivity. Princeton University Press, 2021.

DAUGMAN, JOHN. The importance of being random: statistical principles of iris recognition. Pattern recognition, v. 36, n. 2, p. 279-291, 2003.

DAVIDE CASTELVECCHI. Is facial recognition too biased to be let loose? Nature, v. 587, n. 7834, p. 347-349, 18 nov. 2020.

DE GOEDE, M. Engagement all way down. Critical Studies on Security, v. 8, n. 2, p. 101-115, 2020.

DE GOEDE, M. Speculative Security: The Politics of Pursuing Suspect Monies. University of Minnesota Press, Minneapolis, 2012.

DE GOEDE, MARIEKE; SULLIVAN, GAVIN. The politics of security lists. Environment and Planning D: Society and Space, v. 34, n. 1, p. 67-88, 2016.

DE GOEDE, MARIEKE. The politics of privacy in the age of preemptive security: Introduction. International Political Sociology, v. 8, n. 1, p. 100-104, 2014.

DE SIQUEIRA, ISABEL. Development by trial and error: the authority of good enough numbers. International Political Sociology, v. 11, n. 2, p. 166-184, 2017.

DE LA BELLACASA, Maria Puig. Matters of care: Speculative ethics in more than human worlds. U of Minnesota Press, 2017.

DE SIQUEIRA, ISABEL ROCHA. Measuring and Managing 'fragile States': Quantification and Power. Tese de Doutorado. King's College London, 2014.

DELEUZE, G. El Bergsonismo. Trad. Luis Ferrero Carracedo. Madri: Cátedra, 1987.

DEN, V. Virtual Borders: International Law and the Elusive Inequalities of Algorithmic Association. European Journal of International Law, 11 maio 2022.

DENTON, E. et al. Bringing the People Back In: Contesting Benchmark Machine Learning Datasets. Disponível em: https://arxiv.org/abs/2007.07399. Acesso em: 26 dez. 2023.

DERRIDA, J. Força de Lei: o fundamento místico da autoridade. São Paulo: Martins Fontes, 2007.

DESROSIÈRES, ALAIN. The politics of large numbers: A history of statistical reasoning. Harvard University Press, 1998.

DIAKOPOULOS, NICHOLAS. Accountability in algorithmic decision making. Communications of the ACM, v. 59, n. 2, p. 56-62, 2016.

DIXON, PAM. A Failure to “Do No Harm”--India’s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US. Health and technology, v. 7, n. 4, p. 539-567, 2017.

DONEDA, D.; ALMEIDA, V. O que é governança de algoritmos? In: BRUNO et al. (org.). Tecnopolíticas da Vigilância: perspectivas da margem. 1. ed. São Paulo: Boitempo, 2018.

DOYLE, SEAN. Quality management in forensic science. Academic Press, 2018.

DRYER, THEODORA. Algorithms under the Reign of Probability. IEEE Annals of the History of Computing, v. 40, n. 1, p. 93-96, 2018.

DRYER, THEODORA. Designing Certainty: The Rise of Algorithmic Computing in an Age of Anxiety 1920-1970. University of California San Diego, 2019.

EBRAHIMJI, A.; JONES, J. A Black man was misidentified arrested and held for 6 days in place of a White felon twice his age. Disponível em: https://edition.cnn.com/2022/01/27/us/nevada-man-jailed-misidentified-lawsuit/index.html. Acesso em: 22 mar. 2024.

EDWARDS, PAUL N. The closed world: Computers and the politics of discourse in Cold War America. MIT press, 1996.

ELBE, STEFAN; BUCKLAND-MERRETT, GEMMA. Entangled security: Science co-production and intra-active insecurity. European Journal of International Security, v. 4, n. 2, p. 123-141, 2019.

EUBANKS, VIRGINIA. Automating inequality: How high-tech tools profile police and punish the poor. St. Martin's Press, 2018.

EVANS, SAM WEISS; LEESE, MATTHIAS; RYCHNOVSKÁ, DAGMAR. Science technology security: Towards critical collaboration. Social Studies of Science, v. 51, n. 2, p. 189-213, 2021.

EXECUTIVE OFFICE OF THE PRESIDENT PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY. Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf. Acesso em: 10 set. 2023.

EXPOSING THE SECRETIVE COMPANY AT THE FOREFRONT OF FACIAL RECOGNITION TECHNOLOGY. Disponível em: https://www.npr.org/2023/09/28/1202310781/exposing-the-secretive-company-at-the-forefront-of-facial-recognition-technology. Acesso em: 29 out. 2023.

EYEWITNESS MISIDENTIFICATION - Innocence Project. Disponível em: https://innocenceproject.org/eyewitness-misidentification/ . Acesso em: 4 abr. 2024.

FACE RECOGNITION TECHNOLOGY | American Civil Liberties Union. Disponível em: https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology . Acesso em: 11 nov. 2023.

FACE RECOGNITION TECHNOLOGY EVALUATION (FRTE) 1:1 Verification. Disponível em: https://pages.nist.gov/frvt/html/frvt11.html . Acesso em: 31 out. 2023.

FACIAL RECOGNITION TECHNOLOGY: PART II ENSURING TRANSPARENCY IN GOVERNMENT USE HEARING BEFORE THE COMMITTEE ON OVERSIGHT AND REFORM HOUSE OF REPRESENTATIVES ONE HUNDRED SIXTEENTH CONGRESS FIRST SESSION. Disponível em:

https://docs.house.gov/meetings/GO/GO00/20190604/109578/HHRG-116-GO00-Transcript-20190604.pdf . Acesso em: 8 nov. 2023.

FELDSTEIN, S. The Global Expansion of AI Surveillance. Disponível em: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 . Acesso em: 5 maio. 2024.

FERGUNSON, ANDREW GUTHRIE. Illuminating Black Data Policing. Ohio St. J. Crim. L., v. 15, p. 503, 2017.

FERGUNSON, ANDREW GUTHRIE. The rise of big data policing: Surveillance race and the future of law enforcement. NYU Press, 2017.

FLORIDI, LUCIANO. AI and its new winter: From myths to realities. Philosophy & Technology, v. 33, n. 1, p. 1-3, 2020.

FLUSSER, VILÉM. Towards a Philosophy of Photography. Trad. Anthony Mathews. London: Reaktion, 2000.

FONSECA, CLAUDIA LEE WILLIAMS; MACHADO, HELENA. Ciência identificação e tecnologias de governo. Editora da UFRGS, 2015.

FORNENSTIC GENETICS POLICY INITIATIVE. Establishing best practice for forensic DNA databases. Disponível em: http://dnapolicyinitiative.org/report/. Acesso em: 10 set. 2023.

FORSYTH, DAVID A.; PONCE, JEAN. Computer vision: a modern approach. Pearson, 2012.

FOUCAULT, M. Em defesa da sociedade (Curso no Collège de France 1975-1976). São Paulo: Martins Fontes, 2005.

FOUCAULT, M. Is it really important to think? an interview translated by Thomas Keenan. Philosophy & Social Criticism, v. 9, n. 1, p. 30-40, 1982.

FOUCAULT, M. Segurança território e população. Cursos do College de France (1977-1978). São Paulo: Martins Fontes, 2008.

FOUCAULT, M.; Microfísica do poder. 24. ed. RJ: Graal, 2007.

FOUCAULT, MICHEL. Questions of method. In: THE FOUCAULT EFFECT: Studies in governmentality. v. 74, 1991.

FOUCAULT, MICHEL. Ditos & Escritos. Genealogia da ética subjetividade e sexualidade (vol. IX). Rio de Janeiro: Forense Universitária, 2014.

FRENCH, M.; SMITH, G. Surveillance and embodiment: Dispositifs of capture. Body & Society, v. 22, n. 2, 2016.

FRONTLINE. In the Age of AI. Disponível em: https://podcasts.apple.com/de/podcast/frontlinefilm-audio-track-pbs/id336934080?l=en&i=1000456779283 . Acesso em: 19 out. 2023.

FULLER, M.; GOFFEY, A. Evil Media. MIT Press, Cambridge MA, 2012.

FULLER, STEVE. Faith and reason in an age of humanity 2.0: revisiting cybernetics as 'artificial theology'. Existential Analysis, v. 23, n. 2, p. 212-220, 2012.

FUSSELL, S. An Algorithm That "Predicts" Criminality Based on a Face Sparks a Furor. Disponível em: https://www.wired.com/story/algorithm-predicts-criminality-based-face-sparks-furor/. Acesso em: 20 maio. 2024.

FUSSEY, PETE; DAVIES, BETHAN; INNES, MARTIN. 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. The British journal of criminology, v. 61, n. 2, p. 325-344, 2021.

FUSSEY, Peter; MURRAY, Daragh. Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. 2019.

GALISON, P. Image and Logic: A Material Culture of Microphysics. Chicago: University of Chicago Press, 1997.

GARVIE, C. Garbage in, garbage out: Face recognition on flawed data. Georgetown Law Center on Privacy & Technology. 2019.

GARVIE, Clare, A Forensic Without the Science: Face Recognition in U.S. Criminal Investigations, Center on Privacy & Technology at Georgetown Law. 2022.
GARLAND, D. The culture of control: Crime and social order in contemporary society. Chicago: The University of Chicago Press, 2001.

GERSHGORN, D. Is there any way out of Clearview's facial recognition database? Disponível em: https://www.theverge.com/22522486/clearview-ai-facial-recognition-avoid-escape-privacy. Acesso em: 10 nov. 2023.

GILLESPIE, T. The relevance of algorithms. Media technologies: Essays on communication materiality and society, p. 167, 2014.

GILLESPIE, Tarleton. The politics of 'platforms'. New media & society 12, no. 3 (2010): 347-364.

GILLIS, W. Disponível em: https://www.thestar.com/news/gta/144-toronto-police-officers-signed-up-to-use-clearview-ai-mass-surveillance-tech/article_2cf7befc-7c22-5b47-bcb7-ab365d426569.html. Acesso em: 30 ago. 2023.

GITELMAN, LISA et al. Data bite man: The work of sustaining a long-term study, p. 147-166, 2013.

GOFFEY, A (2008) Algorithm. In: M Fuller (ed) Software Studies. A Lexicon, pp. 15– 20. MIT Press, Cambridge, MA

GOLDENFEIN, JAKE. Facial Recognition is Only the Beginning. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3546525. Acesso em: 10 nov. 2021.

GOLDENFEIN, Jake. "The profiling potential of computer vision and the challenge of computational empiricism." Proceedings of the Conference on Fairness, Accountability, and Transparency. 2019.
Goriunova

GORIUNOVA, OLGA. Face abstraction! Biometric identities and authentic subjectivities in the truth practices of data. Subjectivity, v. 12, n. 1, p. 12-26, 2019.

GRANJA, H. GENÉTICA FORENSE E GOVERNANÇA DA CRIMINALIDADE. Disponível em: https://www.cfbdadosadn.pt/Documents/Fundo%20Documental/Livro_GeneticaForense.pdf. Acesso em: 10 set. 2023.

HAACK, SUSAN. Legal Probabilism: An Epistemological Dissent. In: Evidence Matters: Science Proof and Truth in the Law. Cambridge: Cambridge University Press, 2014, p. 61.

HACKING, I. Making up people. In: BIAGIOLI, M. (ed.). The Science Studies Reader. New York: Routledge, p. 161-171, 1999.

HACKING, I. The emergence of probability: A philosophical study of early ideas about probability induction and statistical inference. Cambridge University Press, 2006.

HACKING, IAN. The taming of chance. Cambridge University Press, 1990.

HACKING, IAN. The Social Construction of What. Cambridge Massachusetts and London England: Harvard University Press, 1999.

HACKING, IAN. 'Language truth and reason'30 years later. Studies in History and Philosophy of Science Part A, v. 43, n. 4, p. 599-609, 2012.

HACKING, Ian. "'Language, truth and reason'30 years later." Studies in History and Philosophy of Science Part A 43.4 (2012): 599-609.

HACKING, Ian. "Kinds of people: Moving targets." Proceedings-British Academy. Vol. 151. OXFORD UNIVERSITY PRESS INC., 2007.

HACKING, Ian. All kinds of possibility. The Philosophical Review, v. 84, n. 3, p. 321-337, 1975.

HACKING, Ian. Styles of scientific thinking or reasoning: A new analytical tool for historians and philosophers of the sciences. Trends in the Historiography of Science (1994): 31-48.

HADDAD, GABRIELLE M. Confronting the biased algorithm: the danger of admitting facial recognition technology results in the courtroom. Vand. J. Ent. & Tech. L., v. 23, p. 891, 2020.

HAGERTY, A. In Ukraine Identifying the Dead Comes at a Human Rights Cost. Disponível em: https://www.wired.com/story/russia-ukraine-facial-recognition-technology-death-military/. Acesso em: 3 nov. 2023.

HALDER, ROHIT et al. Deep learning-based smart attendance monitoring system. Proceedings of the Global AI Congress, 2019. Springer Singapore, 2020.

HANNAH-MOFFAT, K. Algorithmic risk governance: Big data analytics race and information activism in criminal justice debates. Theoretical Criminology, v. 23, n. 4, p. 453-470, 2019.

HANNAH-MOFFAT, Kelly. Actuarial sentencing: An "unsettled" proposition. **Justice quarterly**, v. 30, n. 2, p. 270-296, 2013.

HARAWAY, D. J. Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. Feminist Studies, v. 14, n. 3, p. 575-599, 1988.

HARAWAY, D. J. Staying with the Trouble: Making Kin in the Chthulucene. Durham: Duke University Press, 2016.

HARAWAY, D. The actors are cyborg nature is coyote and the geography is elsewhere: postscript to 'cyborgs at large'. Technoculture, v. 3, p. 183-202, 1991.

HARAWAY, DONNA J.; GOODEVE, THYRZA NICHOLS. Fragmentos: quanto como uma folha. Entrevista com Donna Haraway. Mediações-Revista de Ciências Sociais, v. 20, n. 1, p. 48-68, 2015.

HARAWAY, DONNA. The Promises of Monsters: A Regenerative Politics for Inapproriate/d others. In: The Haraway Reader, p. 63-121. New York: Routledge, 2004.

HARAWAY, DONNA. A manifesto for cyborgs: Science technology and socialist feminism in the 1980s. Australian Feminist Studies, v. 2, n. 4, p. 1-42, 1987.

HARVEY, A. Exposing.ai. Disponível em: https://exposing.ai/. Acesso em: 26 dez. 2023.

HARWELL, D. Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement. Disponível em: https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition/. Acesso em: 11 nov. 2023.

HASKINS, C. The NYPD Has Misled The Public About Its Use Of Facial Recognition Tool Clearview AI. Disponível em: https://www.buzzfeednews.com/article/carolinehaskins1/nypd-has-misled-public-about-clearview-ai-use . Acesso em: 29 out. 2023.

HASKINS, C.; MAC, R.; MCDONALD, L. Instagram-Scraping Clearview AI Wants To Sell Its Facial Recognition Software To Authoritarian Regimes. Disponível em: <https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22?bfsource=relatedmanual>. Acesso em: 3 nov. 2023.

HAWKINSON, K. In every reported false arrests based on facial recognition, that person has been Black. Disponível em: <https://www.businessinsider.com/in-every-reported-false-arrests-based-on-facial-recognition-that-person-has-been-black-2023-8>. Acesso em: 18 jan. 2024.

HAYLES, N. Katherine. "The condition of virtuality." The digital dialectic: New essays on new media (1999): 68-95.

HAYLES, N. Katherine. Traumas of code. Critical Inquiry, v. 33, n. 1, p. 136-157, 2006.

HAYLES, N. Katherine. Computing the human. Theory, Culture & Society, v. 22, n. 1, p. 131-151, 2005.

HAYLES, N. Katherine. How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics. 1987.

HEIDEGGER, Martin. Kant and the Problem of Metaphysics, enlarged. Indiana University Press, 1997.

HILDEBRANDT, Mireille. Criminal law and technology in a data-driven society. In: **The Oxford handbook of criminal law**. Oxford: Oxford University Press, 2014. p. 175-198.

Hill K. The secretive company that might end privacy as we know it. New York Times. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html . 2020. Accessed 18 Jan 2020

HILL, K. Clearview AI App Could End “Privacy As We Know It”. Disponível em: https://www.rollingstone.com/culture/culture-features/clearview-ai-app-privacy-your-face-belongs-to-us-excerpt-1234829211/ . Acesso em: 27 out. 2023.

HODOR-LEE, A. Privacy expert Clare Garvie explains why your face is already in a criminal lineup. Disponível em: https://www.documentjournal.com/2020/10/privacy-expert-clare-garvie-explains-why-your-face-is-already-in-a-criminal-lineup/. Acesso em: 21 jan. 2024.

HONG, SUN-HA. Technologies of Speculation. New York University Press, 2020.

HOOD, JACOB. Making the body electric: The politics of body-worn cameras and facial recognition in the United States. Surveillance & Society, v. 18, n. 2, p. 157-169, 2020.

HOSH, W. L. Machine learning. Encyclopedia Britannica, 2 jun. 2020. Disponível em: https://www.britannica.com/technology/machine-learning .

HU, LILY. Justice beyond utility in artificial intelligence. Proceedings of the 2018 AAAI/ACM Conference on AI Ethics and Society, 2018.

HUMPHRIES, PAUL DOUGLAS. The war on terror in postmodern memory: Explanation understanding and myth in the wake of 9/11. Georgetown University, 2014.

HURLBUT, J. BENJAMIN et al. Bioconstitutional Imaginaries and the Comparative Politics of Genetic Self-knowledge. Science Technology & Human Values, v. 45, n. 6, p. 1087-1118, 2020.

HUYSMANS, J. Security Unbound. Routledge, London, 2014.

HUYSMANS, J. What's in an Act: On Security Speech Acts and Little Security Nothings. Security Dialogue, v. 42, n. 4-5, p. 371-383, 2011.

HUYSMANS, J.; NOGUEIRA, J. P. Ten Years of IPS: Fracturing IR. International Political Sociology, v. 10, n. 4, p. 299-319, 2016.

INTERPOL. Global DNA profiling survey results, 2016. Lyon, 2016.

INTERNATIONAL STANDARDS ORGANIZATION. "Information technology — Vocabulary — Part 37: Biometrics. 2007. https://www.iso.org/standard/66693.html .

INTRONA, L. D. Maintaining the reversibility of foldings: Making the ethics (politics) of information technology visible. Ethics and Information Technology, v. 9, n. 1, p. 11-25, 2007.

INTRONA, LUCAS; WOOD, DAVID. Picturing algorithmic surveillance: The politics of facial recognition systems. Surveillance & Society, v. 2, n. 2-3, p. 177-198, 2004.

ISIN, ENGIN; RUPPERT, EVELYN. The birth of sensory power: How a pandemic made it visible?. Big Data & Society, v. 7, n. 2, p. 2053951720969208, 2020.

JAIN, ANIL K.; ROSS, ARUN. Bridging the gap: from biometrics to forensics. Philosophical Transactions of the Royal Society B: Biological Sciences, v. 370, n. 1674, p. 20140254, 2015.

JASANOFF S, KIM S-H (2009) Containing the atom: sociotechnical imaginaries and nuclear power in the United States and South Korea. Minerva 47(2):119–146.

JASANOFF, S. Containing the atom: sociotechnical imaginaries and nuclear power in the United States and South Korea. Minerva, v. 47, n. 2, p. 119-146, 2009.

JASANOFF, S. Just evidence: The limits of science in the legal process. Journal of Law Medicine & Ethics, v. 34, n. 2, p. 328-341, 2006.

JASANOFF, Sheila. The eye of everyman: Witnessing DNA in the Simpson trial. Social Studies of Science, v. 28, n. 5-6, p. 713-740, 1998.

JASANOFF, Sheila. Judgment under siege: The three-body problem of expert legitimacy. In: Democratization of expertise? Exploring novel forms of scientific advice in political decision-making. Dordrecht: Springer Netherlands, 2005. p. 209-224.

JASANOFF, S. Science at the bar. Law science and technology in America. Cambridge MA and London UK: Harvard University Press, 1995.

JASANOFF, S. ed. States of Knowledge: The Co-Production of Science and Social Order. London: Routledge, 2004.

JASANOFF, S.; SIMMET, HILTON R. No funeral bells: Public reason in a 'post-truth'age. Social studies of science, v. 47, n. 5, p. 751-770, 2017.

JASANOFF, Sheila. "One. Future Imperfect: Science, Technology, and the Imaginations of Modernity." Dreamscapes of modernity. University of Chicago Press, 2015. 1-33.

JASANOFF, Sheila. "Virtual, visible, and actionable: Data assemblages and the sightlines of justice." Big Data & Society 4.2 (2017): 2053951717724477.

JIN, ANGELA; SALEHI, NILOUFAR. (Beyond) Reasonable Doubt: Challenges that Public Defenders Face in Scrutinizing AI in Court. arXiv preprint arXiv:2403.13004, 2024.

JOHNS, F. Global Governance through the Pairing of List and algorithm. Environment and Planning D, v. 34, n. 1, p. 126-149, 2016.

JOHNSON, K. FBI Agents Are Using Face Recognition Without Proper Training. Disponível em: https://www.wired.com/story/fbi-agents-face-recognition-without-proper-training/?utm_source=twitter&mbid=social_tw_sci&utm_social-type=owned&utm_medium=social&utm_brand=wired-science . Acesso em: 5 out. 2023.

JOHNSON, K. How Wrongful Arrests Based on AI Derailed 3 Men's Lives. Disponível em: https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ . Acesso em: 10 abr. 2024.

JOHNSON, T. L.; et al. Facial recognition systems in policing and racial disparities in arrests. Government Information Quarterly, v. 39, n. 4, p. 101753-101753, 1 out. 2022.

KAUFMANN, MAREILE. Who connects the dots?: Agents and agency in predictive policing. In: Technology and agency in international relations. Taylor & Francis, 2019.

KAUFMANN, MAREILE; TZANETAKIS, MEROPI. Doing Internet research with hard-to-reach communities: methodological reflections on gaining meaningful access. Qualitative Research, v. 20, n. 6, p. 927-944, 2020.

KAYNE, D. H. Identification, individualization, uniqueness. Law, Probability and Risk, 8(2), 85-94. 2009

KHAN, PROTIMA et al. Machine learning and deep learning approaches for brain disease diagnosis: principles and recent advances. IEEE Access, v. 9, p. 37622-37655, 2021.

KITCHIN, R. The data revolution: Big Data open data data infrastructures and their consequences. London: Sage, 2014.

KITCHIN, R. Thinking critically about and researching algorithms. Information Communication and Society, v. 20, n. 1, p. 14-29, 2017.

KNORR-CETINA, K. Epistemic cultures. How the sciences make knowledge. Cambridge MA; London UK: Harvard University Press, 1999.

KRUSE, C. The social life of forensic evidence. Oakland CA: University of California Press, 2016.

KUHN, T. Revoluções Científicas. São Paulo: Perspectiva, 1978.

LATOUR, B. An introduction to actor-network-theory. Reassembling the Social, 2005.

LATOUR, B. Science in action: How to follow scientists and engineers through society. Harvard University Press, 1987.

LATOUR, B. The making of law: An ethnography of the Conseil d'Etat. Polity, 2010.

LATOUR, B.; WOOGAR, STEVE. Vida de laboratório: a produção dos fatos científicos. Rio de Janeiro: Relume-Dumará, 1997.

LATOUR. B. La fabrique du droit: Une ethnographie du Conseil d'État, Collection Sciences Humaines et Sociales, Éditions La Découverte Poche, Paris, 2004.

LAW ENFORCEMENT FACIAL RECOGNITION USE CASE CATALOG Law Enforcement Imaging Technology Task Force. A joint effort of the IJIS Institute and the International Association of Chiefs of Police. Disponível em: https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf . Acesso em: 10 set. 2023.

LEANDER, ANNA; WÆVER, OLE (Ed.). Assembling exclusive expertise: knowledge ignorance and conflict resolution in the global South. Routledge, 2018.

LEANDER, A. 'The Promises, Problems, and Potentials of a Bourdieu-Inspired Staging of International Relations', International Political Sociology 5: 3 (2011), 294-313.

LE CUN, YANN; BENGIO, YOSHUA; HINTON, GEOFFREY. Deep learning. Nature, v. 521, n. 7553, p. 436-444, 2015.

LEESE, M. The New Profiling. Security Dialogue, v. 45, n. 5, p. 494-511, 2014.

LOFRED, MADZOU et al. Best practice for facial recognition in law enforcement. Disponível em: https://www.weforum.org/agenda/2021/10/facial-recognition-technology-law-enforcement-human-rights/. Acesso em: 3 jan. 2024.

LIPTON, B. GAO Report Shows the Government Uses Face Recognition with No Accountability Transparency or Training. Disponível em: https://www.eff.org/deeplinks/2023/10/gao-report-shows-government-uses-face-recognition-no-accountability-transparency. Acesso em: 12 out. 2023.

LISLE, Debbie. Failing worse? Science security and the birth of a border technology. European Journal of International Relations, v. 24, n. 4, p. 887-910, 2018.

LOFRED MADZOU et al. Best practice for facial recognition in law enforcement. Disponível em: <https://www.weforum.org/agenda/2021/10/facial-recognition-technology-law-enforcement-human-rights/>. Acesso em: 3 jan. 2024.

LYNCH, M. God's signature: DNA profiling, the new gold standard in forensic science. Endeavour, 27(2), 93-97. 2003

LYNCH, Michael, and Ruth MACNALLY. "Forensic DNA databases and biolegality: the co-production of law, surveillance technology and suspect bodies." The Handbook of Genetics & Society. Routledge, 2009. 309-327.

LYNCH, Michael. Science, truth, and forensic cultures: The exceptional legal status of DNA evidence. Studies in History and Philosophy of Science Part C: Studies in History and Philosophy of Biological and Biomedical Sciences, v. 44, n. 1, p. 60-70, 2013.

LYNCH, Michael; COLE, Simon. Science and Technology Studies on Trial:: Dilemmas of Expertise. In: Expert Evidence and Scientific Proof in Criminal Trials. Routledge, 2017. p. 49-91.

LYON, David. "Biometrics, identification and surveillance." Bioethics 22.9: 499-508. 2008.

LYON, David. Surveillance society: Monitoring everyday life. McGraw-Hill Education (UK), 2001

MAC, R.; HASKINS, C.; MCDONALD, L. **Clearview AI Says It Identified A Terrorism Suspect. The Cops Say That's Not True.** Disponível em: <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-nypd-facial-recognition?bfsource=relatedmanual>. Acesso em: 31 out. 2023.

MAC, R.; HASKINS, C.; MCDONALD, L. **Clearview AI's Facial Recognition Tech Is Being Used By The Justice Department, ICE, And The FBI**. Disponível em: <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>. Acesso em: 31 out. 2023.

MACHADO, H., & PRAINSACK, B. Tracing technologies: Prisoners' views in the era of CSI. Farnham, UK: Ashgate.2012.

MACHADO, H., Granja, R., & AMELUNG, N. Constructing suspicion through forensic DNA databases in the EU. The views of the Prüm professionals. The British Journal of Criminology, 60(1), 141-156.2020.

MACHADO, H. G. GENÉTICA FORENSE E GOVERNANÇA DA CRIMINALIDADE. Disponível em: https://www.cfbdadosadn.pt/Documents/Fundo%20Documental/Livro_GeneticaForense.pdf. Acesso em: 10 set. 2023.

MCCLOCH, Jude; Pickering, Sharon. Pre-Crime and Counter-TerrorismImagining Future Crime in the 'War on Terror'. The British Journal of Criminology, v. 49, n. 5, p. 628-645, 2009.

MCGOY, Linsey (Ed.). An introduction to the sociology of ignorance: essays on the limits of knowing. Routledge, 2016.

MCKAY, T. Clearview AI Says It Can Do the "Computer Enhance" Thing. Disponível em: <https://gizmodo.com/clearview-ai-says-it-can-do-the-computer-enhance-thin-1847795776>. Acesso em: 11 nov. 2023.

MCQUILLIAN, Dan. Algorithmic paranoia and the convivial alternative. Big Data & Society, v. 3, n. 2, p. 2053951716671340, 2016.

MCSORLEY, Tim. "The Case for a Ban on Facial Recognition Surveillance in Canada." Surveillance & Society 19.2 (2021): 250-254.

MATTSON, J. Algorithmic risk governance: Big data analytics race and information activism in criminal justice debates. Theoretical Criminology, v. 23, n. 4, p. 453-470, 2019.

MARTINS, L. Exclusivo: Clearview ofereceu fotos de brasileiros para polícias e Ministério da Justiça. Disponível em: <https://www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/>. Acesso em: 11 nov. 2023.

MATZNER, T. (2016). Beyond data as representation: The performativity of Big Data in surveillance. Surveillance & Society, 14(2), 197-210.

MAULUD, Dastan, and Adnan M. Abdulazeez. "A Review on Linear Regression Comprehensive in Machine Learning." Journal of Applied Science and Technology Trends 1.4 (2020): 140-147.

MAY, S. A Failure to "Do No Harm"--India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US. Health and Technology, v. 7, n. 4, p. 539-567, 2017.

MAYER-SCHONBERG, V., & Cukier, K. Big Data: a revolution that will transform how we live, work, and think (p. 73-97). Hoghton Mifflin Harcourt: New York. 2013.

MENDONÇA, TIAGO. Machine Learning sob a ótica estatística. Ufscar/Insper, 2018.

MELAMED, S. Philly police use of Clearview AI was just "a test" — but facial recognition is already here. Disponível em: <https://www.inquirer.com/news/clearview-ai-

philadelphia-police-department-facial-recognition-20200305.html>. Acesso em: 20 jan. 2024.

METZ, R. First, they banned facial recognition. Now they're not so sure. Disponível em: <https://edition.cnn.com/2022/08/05/tech/facial-recognition-bans-reversed/index.html>. Acesso em: 5 jan. 2024.

MITTELSTADT, Brent Daniel et al. The ethics of algorithms: Mapping the debate. Big Data & Society, v. 3, n. 2, p. 2053951716679679, 2016.

MOL, A. 2002. The Body Multiple: Ontology in Medical Practice. Durham NC: Duke University.

MONSSES, Linda. Public relations: Theorizing the contestation of security technology. Security Dialogue, v. 50, n. 6, p. 531-546, 2019.

MOY, Timothy. War Machines: Transforming Technologies in the U.S. Military, 1920-1940 (Texas A & M University military history series; 71). 1st ed. Texas A&M University Press, 2001.

NACDL - Challenging Facial Recognition Software in Criminal Court. Disponível em: <https://www.nacdl.org/Article/July2019-ChallengingFacialRecognitionSoftwareinCri>. Acesso em: 11 abr. 2024.

NAGPAL, Shruti, et al. "Deep learning for face recognition: Pride or prejudiced?." arXiv preprint arXiv:1904.01219 (2019).

NAIR, Vijayanka. "Becoming data: biometric IDs and the individual in 'Digital India'." Journal of the Royal Anthropological Institute 27.S1 (2021): 26-42.

NANNA BONDE THYLSTRUP. The ethics and politics of data sets in the age of machine learning: deleting traces and encountering remains - Nanna Bonde Thylstrup, 2022. Disponível em: <https://journals.sagepub.com/doi/10.1177/01634437211060226>. Acesso em: 26 dez. 2023.

NASEEM, Imran, Roberto TOGNERI, and Mohammed BENNAMOUN. "Linear regression for face recognition." IEEE transactions on pattern analysis and machine intelligence 32.11 (2010): 2106-2112.

NATALE, Simone, and Andrea BALLATORE. "Imagining the thinking machine: Technological myths and the rise of artificial intelligence." Convergence 26.1 (2020): 3-18.

NUNES, Pablo; LIMA, Thallita Gabriele Lopes; CRUZ, Thaís Gonçalves. O SERTÃO VAI VIRAR MAR: Expansão do reconhecimento facial na Bahia. Rio de Janeiro: CESeC, 2023.

O'BRIEN, L. **The Far-Right Helped Create The World's Most Powerful Facial Recognition Technology**. Disponível em: <https://www.huffingtonpost.co.uk/entry/clearview-ai-facial-recognition-alt-right_n_5e7d028bc5b6cb08a92a5c48?ri18n=true&guccounter=1>. Acesso em: 29 out. 2023.

O’GRANDY, Nathaniel. Automating security infrastructures: Practices, imaginaries, politics. Security Dialogue, p. 0967010620933513, 2020.

O’NEIL, C. The era of blind faith in big data must end. TIW Spreading (ed.), 2017a

O’NEIL, C. Weapons of math destruction: How big data increases inequality and threatens democracy. Broadway Books. 2017b.

OROZCO, Alex Mulattieri Suarez et al. Balanceamento entre segurança e desempenho na comunicação entre os planos de controle e dados em redes definidas por software. 2018.

Overview | Clearview AI. Disponível em: <https://www.clearview.ai/overview>. Acesso em: 28 out. 2023.

PARENTI, C. 2003. The Soft Cage: Surveillance in America from Slavery Passes to War on Terror. New York: Basic Books: 50. 2003.

PARISI, Luciana. Speculation: a method for the unattainable. In: Inventive Methods. Routledge, 2012. p. 246-258.

PARISI, Luciana. Contagious architecture: Computation, aesthetics, and space. mit Press, 2013.

PARISI, Luciana. Critical computation: Digital automata and general artificial thinking. Theory, Culture & Society, v. 36, n. 2, p. 89-121, 2019.

Parks v. McCormac | American Civil Liberties Union. Disponível em: <https://www.aclu.org/cases/parks-v-mccormac>. Acesso em: 10 abr. 2024.

PASQUALE, Frank. The black box society. Harvard University Press, 2015.

PERRITT JR, Henry H. Defending Face-Recognition Technology (and Defending against It). J. Tech. L. & Pol'y, v. 25, p. 41, 2020.

PEW RESEARCH CENTER. **2. Public more likely to see facial recognition use by police as good, rather than bad for society**. Disponível em: <https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-society/>. Acesso em: 1 mar. 2024.

PFTENHAUER, Sebastian, and Sheila JASANOFF. "Traveling imaginaries: The “practice turn” in innovation policy and the global circulation of innovation models." The Routledge handbook of the political economy of science. Routledge, 2017. 416-428.

PONCE, JEAN; FORSYTH, DAVID A. Computer vision: a modern approach. Pearson, 2012.

PORTER, T. M. Trust in numbers: The pursuit of objectivity in science and public life. Princeton, NJ: Princeton University Press.1995.

PRESIDENT’S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY. Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison

Methods. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf . Acesso em: 10 set. 2023.

PRESS, E. **Does A.I. Lead Police to Ignore Contradictory Evidence?** Disponível em: <https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence>. Acesso em: 13 abr. 2024.

PUAR, J. K. *Terrorist assemblages: Homonationalism in queer times*. Durham: Duke University Press. 2007.

PUGLIESE, Joseph. Biometrics: Bodies, technologies, biopolitics. Routledge, 2010.

RABINOW, P. Artificiality and enlightenment: From sociobiology to biosociality. In Essays on the anthropology of reason (pp. 91-111). Princeton, NJ: Princeton University Press. 1996.

RADINA STOYKOVA. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. **Computer Law & Security Review**, v. 42, p. 105575–105575, 1 set. 2021.

RAJI, Inioluwa Deborah, et al. "Saving face: Investigating the ethical concerns of facial recognition auditing." Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society. 2020.

RANCIÈRE, Jacques. A few remarks on the method of Jacques Rancière. parallax, v. 15, n. 3, p. 114-123, 2009.

RANCIÈRE, Jacques. The emancipated spectator. Verso Books, 2021.

RAVIV, Shaun. “The Secret History of Facial Recognition.” Wired, January 21, 2020. https://www.wired.com/story/secret-history-facial-recognition . (Accessed December 12, 2021).

REASON, S. A Failure to “Do No Harm”--India’s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the US. Health and Technology, v. 7, n. 4, p. 539-567, 2017.

REED, Clare. "Written evidence." A Rape of the Soul so Profound. Routledge, 2020. 17-45.

REEDY, Paul. Interpol review of digital evidence 2016-2019. **Forensic Science International: Synergy**, v. 2, p. 489-520, 2020.

REZENDE, Isadora Neroni. "Facial recognition in police hands: Assessing the ‘Clearview case’from a European perspective." New Journal of European Criminal Law 11.3 (2020): 375-389.

RIGANO, C. **USING ARTIFICIAL INTELLIGENCE TO ADDRESS CRIMINAL JUSTICE NEEDS**. Disponível em: <https://www.ojp.gov/pdffiles1/nij/252038.pdf>.

RISHEL, ANDREW GUTHRIE. Illuminating Black Data Policing. Ohio St. J. Crim. L., v. 15, p. 503, 2017.

ROBERTS, SARAH; BELL, CATHERINE. Taking people apart: Digitised dissection and the body at the border. Environment and Planning D: Society and Space, v. 27, n. 3, p. 444-464, 2009.

ROBERTS, Paul, and Michael STOCKDALE, eds. Forensic Science Evidence and Expert Witness Testimony: Reliability Through Reform?. Edward Elgar Publishing, 2018.

ROGERS, J.; MCGUIRE, D. The politics of security lists. Environment and Planning D: Society and Space, v. 34, n. 1, p. 67-88, 2016.

ROSE, N. The politics of life itself: Biomedicine, power, and subjectivity in the twenty--first century. Princeton: Princeton University Press. 2007.

ROSE, N.; NOVAS, C. (2005). Biological citizenship. In S. J. Collier & A. Ong (Eds.), Global assemblages: Technology, politics, and ethics as anthropological problems (pp. 439-463). Malden, MA: Blackwell Publishers.

ROUVROY, Antoinette. The end (s) of critique: Data behaviourism versus due process. In: Privacy, due process and the computational turn. Routledge, 2013. p. 143-165.

ROUVROY, A.; BERNS, T. Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? In: BRUNO et al. (org.). Tecnopolíticas da Vigilância: perspectivas da margem. 1. Ed. São Paulo: Boitempo, 2018.

RUPPERT, Evelyn; ISIN, Engin; BIGO, D. (2017). Data politics. Big Data & Society, v. 4, n. 2, p. 2053951717717

SAFRAN, STEFAN. Global governance through the pairing of list and algorithm. Environment and Planning D, v. 34, n. 1, p. 126-149, 2016.

SAFRAN, STEFAN; ROGERS, J. What's in an Act: On Security Speech Acts and Little Security Nothings. Security Dialogue, v. 42, n. 4-5, p. 371-383, 2011.

SALMON, PATRICIA; ROBERTS, SARAH. Taking people apart: Digitised dissection and the body at the border. Environment and Planning D: Society and Space, v. 27, n. 3, p. 444-464, 2009.

SAUGMANN, Rune. The security captor, captured. Digital cameras, visual politics and material semiotics. Critical Studies on Security, v. 8, n. 2, p. 130-144, 2020.

SAVAGE, KENNETH. Epistemic cultures. How the sciences make knowledge. Cambridge MA; London UK: Harvard University Press, 1999.

SCHNEIDER, KLAUS. Science at the bar. Law science and technology in America. Cambridge MA and London UK: Harvard University Press, 1995.

SEAVER, Nick. "Knowing algorithms." Digital STS (2019): 412-422.

SEAVER, Nick. "What should an anthropology of algorithms do?." Cultural anthropology 33.3 (2018): 375-385.

SHAKER, Z. How We Store and Search 30 Billion Faces. Disponível em: <https://www.clearview.ai/post/how-we-store-and-search-30-billion-faces>. Acesso em: 14 nov. 2023.

SHERRIS, C.; RISHEL, ANDREW GUTHRIE. Illuminating Black Data Policing. Ohio St. J. Crim. L., v. 15, p. 503, 2017.

SIMMONS, K.; ROBERTS, SARAH. Taking people apart: Digitised dissection and the body at the border. Environment and Planning D: Society and Space, v. 27, n. 3, p. 444-464, 2009.

SIMPSON, KATHERINE. Science at the bar. Law science and technology in America. Cambridge MA and London UK: Harvard University Press, 1995.

SIMMLER, M. et al. Smart criminal justice: exploring the use of algorithms in the Swiss criminal justice system. **Artificial Intelligence and Law**, v. 31, n. 2, p. 213–237, 14 mar. 2022.

SINNERBRINK, Robert. Deconstructive Justice and the "Critique of Violence": On Derrida and Benjamin. **Social Semiotics**, v. 16, n. 3, p. 485-497, 2006.

SMITH, GEORGE; MATTSON, J. Algorithmic risk governance: Big data analytics race and information activism in criminal justice debates. Theoretical Criminology, v. 23, n. 4, p. 453-470, 2019.

SMITH, GEORGE; ROBERTS, SARAH. Taking people apart: Digitised dissection and the body at the border. Environment and Planning D: Society and Space, v. 27, n. 3, p. 444-464, 2009.

SMITH, MURRAY; RISHEL, ANDREW GUTHRIE. Illuminating Black Data Policing. Ohio St. J. Crim. L., v. 15, p. 503, 2017.

STAR, SUSAN LEIGH; BOWKER, GEOFFREY. Sorting things out. Classification and its consequences, 1999.

SOCHER, R.; MANNING, C. Deep learning for natural language processing (without magic). In: Keynote at the 2013 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL 2013). 2013.

SOMMER, Peter. Forensic science standards in fast-changing environments. Science & Justice, v. 50, n. 1, p. 12-17, 2010.

STENGERS, Isabelle. The invention of modern science. U of Minnesota Press, 2000.

STENGERS, Isabelle. The invention of modern science. U of Minnesota Press, 2000.

STENGERS, Isabelle; De Sutter, Laurent. Une pratique cosmopolitique du droit est-elle possible?. Entrevista com Laurent de Sutter em Cosmopolitiques, v. 8, 2004.

STENGERS, Isabelle; E SILVA, Fernando Silva; ROQUE, Tatiana. **Uma Outra Ciência é Possível: Manifesto Por Uma Desaceleração das Ciências**. Bazar Do Tempo, 2023.

Stigler, Stephen M. "Francis Galton's account of the invention of correlation." *Statistical Science* (1989): 73-79.

STEYERL, HITO. Free Fall: A Thought Experiment on Vertical Perspective. E-flux Journal, n. 24, p. 1-8, 2011.

STOYKOVA, Radina. A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings. **Available at SSRN 4551317**.

Suchman, Lucy. Algorithmic warfare and the reinvention of accuracy. Critical Studies on Security, v. 8, n. 2, p. 175-187, 2020.

SUCHMAN, Lucy. Algorithmic warfare and the reinvention of accuracy. Critical Studies on Security, v. 8, n. 2, p. 175-187, 2020.

SUCHMAN, Lucy. Located accountabilities in technology production. Scandinavian journal of information systems, v. 14, n. 2, p. 7, 2002.

SUCHMAN, Lucy. Human-machine reconfigurations: Plans and situated actions. Cambridge university press, 2007.

SUCHMAN, Lucy. Technologies of accountability: Of lizards and airplanes. Technology in working order: Studies of work, interaction and technology, p. 113-126, 1992.

SULLIVAN, R.; DE GOEDE, MARIEKE. The politics of security lists. Environment and Planning D: Society and Space, v. 34, n. 1, p. 67-88, 2016.

SVENSÉN, Markus; Bishop, Christopher M. Pattern Recognition and Machine Learning Errata and Additional Comments. 2011.

SZELISKI, Richard. Computer vision: algorithms and applications. Springer Nature, 2022.

TANWAR, Sudeep, et al. "Ethical, legal, and social implications of biometric technologies." Biometric-based physical and cybersecurity systems. Springer, Cham, 2019. 535-569.

Terms of Service | Clearview AI. Disponível em: https://www.clearview.ai/terms-of-service#:~:text=Subject%20to%20the%20terms%20of,uploaded%20to%20the%20Products%20and . Acesso em: 10 nov. 2023.

THIBAUT, B.; SAVAGE, KENNETH. Epistemic cultures. How the sciences make knowledge. Cambridge MA; London UK: Harvard University Press, 1999.

THOMPSON, A. The seductiveness of fairness: Is machine learning the answer?–Algorithmic fairness in criminal justice systems. In: The Algorithmic Society. Routledge, p. 87-103, 2020.

TIMNIT, G.; BUOLAMWINI, JOY. Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on fairness accountability and transparency. PMLR, 2018.

TISTARELLI, Massimo, and Christophe Champod, eds. Handbook of biometrics for forensic science. Springer International Publishing, 2017.

TONI, R.; SIMMONS, K. Taking people apart: Digitised dissection and the body at the border. Environment and Planning D: Society and Space, v. 27, n. 3, p. 444-464, 2009.

TOOSI, Amirhosein, et al. "A brief history of AI: how to prevent another winter (a critical review)." PET clinics 16.4 (2021): 449-469.

TURING, Alan, 'Lecture on the Automatic Computing Engine (1947)', in B J Copeland (ed.), The Essential Turing (Oxford, 2004; online edn, Oxford Academic, 12 Nov. 2020),

ULBRICH, L (2018) When Big Data Meet Securitization. European Journal for Security Research 3(2), 139– 161

VALVERDE, C.; VAN MUNSTER, R. Governing terrorism through risk: Taking precautions (un)knowing the future. European journal of international relations, v. 13, n. 1, p. 89-115, 2007.

VAN DER PLOEG, I. (1999). Written on the body: Biometrics and identity. Computers and Society, March, 37-44.

VAN DIJIK, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, 12(2), 197-208.

VAN DONGEN, Jeroen. "The historical contingency of rationality: The social sciences and the Cold War." (2015): 71-76.

VASQUEZ, D.; SALEHI, NILOUFAR. (Beyond) Reasonable Doubt: Challenges that Public Defenders Face in Scrutinizing AI in Court. arXiv preprint arXiv:2403.13004, 2024.

VOULODIMOS, Athanasios et al. Deep learning for computer vision: A brief review. Computational intelligence and neuroscience, v. 2018, 2018

WALTERS, William. Secrecy, publicity and the milieu of security. Dialogues in human geography, v. 5, n. 3, p. 287-290, 2015

WANG, Jackie. Carceral capitalism. MIT Press, 2018.

WÆVER, OLE. Assembling exclusive expertise: knowledge ignorance and conflict resolution in the global South. Routledge, 2018.

WELSH, R.; MATTSON, J. Algorithmic risk governance: Big data analytics race and information activism in criminal justice debates. Theoretical Criminology, v. 23, n. 4, p. 453-470, 2019.

WELINDER, Yana. "A face tells more than a thousand posts: developing face recognition privacy in social networks." Harv. JL & Tech. 26 (2012): 165.

WEXLER, R. **Defendants Should Have the Right to Inspect the Software Code Used to Convict Them**. Disponível em: <https://slate.com/technology/2015/10/defendants-should-be-able-to-inspect-software-code-used-in-forensics.html>. Acesso em: 5 abr. 2024.

WHELAN, T.; HOBDEN, STEPHEN; KAVALSKI, EMILIAN. Posthuman dialogues in international relations. Routledge, 2017.

WHELAN, T.; SAVAGE, KENNETH. Epistemic cultures. How the sciences make knowledge. Cambridge MA; London UK: Harvard University Press, 1999.

WIENROTH, Matthias. Value beyond scientific validity: let's RULE (Reliability, Utility, LEgitimacy). **Journal of Responsible Innovation**, v. 7, n. sup1, p. 92-103, 2020.

WOOD, DAVID. Picturing algorithmic surveillance: The politics of facial recognition systems. Surveillance & Society, v. 2, n. 2-3, p. 177-198, 2004.

WOOD, DAVID; INTRONA, LUCAS. Picturing algorithmic surveillance: The politics of facial recognition systems. Surveillance & Society, v. 2, n. 2-3, p. 177-198, 2004.

WRIGHT, S. Facial Recognition Technology in Court Cases: Judge Bias in Evaluating FRT Evidence. Disponível em: https://www.aclu.org/report/facial-recognition-technology-court-cases. Acesso em: 14 nov. 2023.

WYNNE, BRIAN. Risk and social learning: Reification to engagement. In: The politics of uncertainty: Managing the unknowns, p. 69-97, 2010.

XIOLIN Wu e XI Zhang, "Automated Inference on Criminality Using Face Images ", arXiv, 13 de novembro2016.

YILUN Wang e Michal KOSIMSKI, "Deep Neural Networks Are More Accurate Than Humans at DetectingSexual Orientation from Facial Images, " Journal of Personality and Social Psychology , vol. 114, nº 2 (2018), p.246.

ZHAO, Wenyi, et al. "Face recognition: A literature survey." ACM computing surveys (CSUR) 35.4 (2003): 399-458.

ZIEGLER, K.; ISIN, ENGIN. The birth of sensory power: How a pandemic made it visible?. Big Data & Society, v. 7, n. 2, p. 2053951720969208, 2020.

ZIEWITZ, M. Governing algorithms: Myth, mess, and methods. Science, Technology & Human Values, 41, 3–16. 2016.