



PROJECT MUSE®

On Facial Recognition, Regulation, and "Data Necropolitics"

Antonio Pele, Caitlin Mulholland

Indiana Journal of Global Legal Studies, Volume 30, Issue 1, 2023, pp.
173-194 (Article)

Published by Indiana University Press



➔ For additional information about this article

<https://muse.jhu.edu/article/886166>

On Facial Recognition, Regulation, and “Data Necropolitics”

ANTONIO PELE & CAITLIN MULHOLLAND*

ABSTRACT

This paper argues for actual and legal regulation of artificial intelligence (AI) and facial recognition. These new technologies represent great opportunities to improve the welfare of societies. However, some of their uses can also enhance discrimination and, eventually, lead to violence. From a comparative approach (examining the European Union and Brazil), we address the current and future aspects of facial regulation, AI, and personal data. This paper shows that regulation is relevant to protect the rule of law, free markets, and individual freedoms. It also examines the looming risks unfolding from the unregulated uses of new technologies. Our concept of “Data Necropolitics” defines a predatory form of digital governance that exploits and discriminates against vulnerable populations.

INTRODUCTION

Increasing literature has been highlighting how our societies and subjectivities are being modified and threatened by new technologies,¹

*Antonio Pele is Associate Professor at the Law School at the Pontifical Catholic University at Rio de Janeiro, Brazil (PUC-Rio), and Marie Curie Fellow EHES/IRIS, Paris (2021–23) with the E.U.-funded project HuDig19. DOI: 10.3030/101027394. Email: apele@puc-rio.br

Caitlin Mulholland is Associate Professor and Head of the Law School at the Pontifical Catholic University at Rio de Janeiro, Brazil (PUC-Rio).
Email : caitlinsm@puc-rio.br

1. See generally Antoinette Rouvroy & Bernard Stiegler, *The Digital Regime of Truth: From Algorithmic Governmentality to a New Rule of Law*, LA DELEUZIANA, no. 3, 2016, at 6; BERNARD E. HARCOURT, EXPOSED: DESIRE AND DISOBEDIENCE IN THE DIGITAL AGE (2015); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); FRANCK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); CÉDRIC DURAND, TECHNO-FÉODALISME - CRITIQUE DE L'ÉCONOMIE NUMÉRIQUE (2020);

Indiana Journal of Global Legal Studies Vol. 30 #1 (Winter 2023)
© Indiana University Maurer School of Law

including “Algorithmic Governmentality” (A. Rouvroy), “Expository Society” (B. Harcourt), “Black Box Society” (F. Pasquale), “Surveillance Capitalism” (S. Zuboff), “Techno-Feudalism”(C. Durand). The present article is inserted in these debates and examines more particularly the role of legal regulation regarding AI and facial recognition. From a comparative approach, it explores the regulation of such fields in Brazil and in Europe. This paper argues that regulation is essential since it is the only way to protect the fundamental basic rights of individuals (e.g., privacy) while avoiding potential discrimination unfolding from socioeconomic and racial biases. Those questions will be addressed in the first part (Part I) of the paper. The second part (Part II) argues that the lack of regulation can lead to violence and, eventually, death. Exploring specific cases where new technologies are related to digital surveillance and military activities, we highlight the dangers of what is called “Data Necropolitics,” namely, a predatory and digital form of governance.

PART I

I. STARTING THE DEBATE: PERSONAL DATA PROTECTION AND ALGORITHMIC NONDISCRIMINATION

In mid-2010, a Taiwanese family purchased a camera from Nikon and found a malfunction.² The product had a feature to prevent selfies with eyes closed, which were confused with the eyes of Asians. As a result, whenever family members tried to photograph each other, a message flashed on the screen asking: “Did someone blink?” This led them to think, at first, that the camera was broken. However, the messages stopped when one of the brothers posed with his eyes wide open. There, it was possible to verify that the intelligent face detection technology, initially designed to make photography more efficient, had a design error that exhibited an occasional bias towards the faces of Caucasians.

Such face detection technology was a feature that quickly gained traction in various smart technological devices. In 2015, Google launched Google Photos, a sharing and storage service designed to provide users free, unlimited photo and video storage. This service applies the technology of markings on images through its AI software

ÉRIC SADIN, *L'INTELLIGENCE ARTIFICIELLE OU L'ENJEU DU SIÈCLE: ANATOMIE D'UN ANTIHUMANISME RADICAL* (2021).

2. Adam Rose, *Are Face-Detection Cameras Racist?*, TIME (Jan. 22, 2010), <http://content.time.com/time/business/article/0,8599,1954643,00.html>.

with the computer vision technique.³ For example, in one of the automatic tagging processes, the application labelled two black men as “gorillas.”⁴ At the time, the company justified the problems in recognizing images due to “obscured faces” and the need for “different contrast processes for different skin tones and lighting,” and presented promises of long-term fixes.⁵

Still, computer vision and facial recognition have been applied in policing several cities around the world. In Brazil, the practice started in December 2018 by the secretary of public security of Bahia in the cities of Feira de Santana and Salvador.⁶ Since its implementation, facial recognition technology has led to approximately 200 arrests in the region.⁷ There were also false positives among the more than 4.3 million recorded images.⁸ For example, a seventeen-year-old teenager was approached inside a subway station to comply with an arrest warrant for drug trafficking. Upon arriving at the police station, police discovered that the boy’s identity was incompatible with the subject identified by the recognition system and that they had apprehended the boy in error.⁹ In another situation, a twenty-five-year-old man with

3. Computer vision is the field of AI that trains computers to interpret and understand the visual world. Depending on programming, machines can identify and classify elements such as objects, animals and people, through images and videos and, together with deep learning models, even react to what they see. In other words, they are systems designed for rapid detection and reaction to visual stimuli. *Computer Vision: What it is and Why it Matters*, SAS, https://www.sas.com/pt_br/insights/analytics/c-computer-vision.html (last visited Jan. 20, 2023).

4. Jana Kasperkevic, *Google Says Sorry for Racist Auto-tag in Photo App*, THE GUARDIAN (July 1, 2015, 1:52 PM), <https://www.theguardian.com/technology/2015/jul/01/google-sorry-racist-auto-tag-photo-app>.

5. *Id.*

6. It works through a comparison system: if the images captured in real-time are more than 90% compatible with those available in the wanted database, alerts are generated to professionals who call teams on the streets to confirm the identity of the suspects and follow up to the execution of the arrest warrant. Marcia Santana, *Facial Recognition Completes One Year and is a National Highlight*, SECRETARIA DE SEGURANÇA PÚBLICA DE ESTADO DA BAHIA (Dec. 18, 2019), <http://www.ssp.ba.gov.br/2019/12/6981/Facial-Recognition-completes-one-year-and-and-national-highlight.html> (Braz.).

7. *Homem é preso em Salvador após ser identificado pelo sistema de reconhecimento facial*, G1 (Mar. 14, 2021, 8:24 AM), <https://g1.globo.com/ba/bahia/noticia/2021/03/14/homem-e-preso-em-salvador-apos-ser-identificado-pelo-sistema-de-reconhecimento-facial.ghtml>.

8. Samuel Celestino, *Facial Recognition System Has Already Recorded More than 4.3 Million Images*, BAHIA NOTÍCIAS (Feb. 24, 2020, 8:00AM), <https://www.bahianoticias.com.br/noticia/244624-sistema-de-reconhecimento-facial-ja-registrou-mais-de-43-milhoes-de-imagens.html> (Braz.).

9. Tarcízio Silva, *Reconhecimento Facial na Bahia: mais erros policiais contra negros e pobres* [*Facial Recognition in Bahia: More Police Errors Against Blacks and the Poor*],

special needs was approached by police forces because the facial recognition system pointed him out as someone with an outstanding arrest warrant.¹⁰

Although such facial recognition technology (FRT) is not a novelty, having already been used in security systems of banking applications and cell phones, for example, the potential of its use for specific purposes—such as investigation and criminal prosecution—has brought about debates over control and surveillance, which takes us back to Bentham and the Panopticon theory,¹¹ and Foucault and his theory on social control and the history of the penitentiary systems.¹²

Machine-learning programs allow the development of facial recognition technology that promotes autonomous decision-making ability free from human interference. It becomes possible through the treatment of bulk data (pictures of people, for example) and self-learning development of machines (i.e., programs and systems) that allow the achievement of specific results (outputs) independently of any mediation by a human being. Such a decision could concretely deny or impede rights or generate abusive or illegitimate discrimination. However, machine-learning applications “are adopting machine-learning systems at unprecedented rates due to the technology’s ability to radically improve data-driven decision-making at a cost and scale incomparable to that of humans.”¹³ As a consequence, their comprehensiveness makes them play an essential role in regulating our lives. For example, the judicial system can use them to assess the probability that a subject will relapse into a particular crime. Banks can decide whether or not an individual should be granted a mortgage. Governments can rely on machine learning to determine market reallocation strategies. It is this scope of situations, and the possible effects their results have generated, that have intensified questions about transparency and accountability.

These questions are natural because those technologies are not easily understandable to humans, especially in the ways they function

TARCÍZIO SILVA (Nov. 21, 2019), <https://tarciziosilva.com.br/blog/reconhecimento-facial-na-bahia-mais-erros-policiais-contranegros-e-pobres> (Braz.).

10. Amanda Palma & Clarissa Pacheco, ‘*O policial já foi com a arma na cabeça dele, diz mãe de rapaz confundido por reconhecimento facial*’ [*The Policeman Already Came with a Gun Pointed to his Head, Says The Mother of a Boy Identified by Facial Recognition*] CORREIO (Jan. 5, 2020, 9:00am), <http://glo.bo/3TFduBt> (Braz.).

11. See JEREMY BENTHAM, *THE PANOPTICON WRITINGS* (Miran Božovič ed., 2011).

12. See MICHEL FOUCAULT, *DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON* 82 (Alan Sheridan trans. 1977).

13. Bryan Casey et al., *Rethinking Explainable Machines: The GDPR’s “Right to Explanation” Debate and the Rise of Algorithmic Audits in Enterprise*, BERKELEY TECH. L.J. 145, 150 (2019).

and how their results are justified. Another concern revealed in the study of algorithms, AI, and facial recognition is the belief that “predictive algorithms rationalize the decision-making process by summarizing all relevant information in a more efficient way than the human brain.”¹⁴ The myth about the objectivity, neutrality, rationality, and impartiality of the application of such technology has been gradually deconstructed. Research has shown that existing biases in human culture are inevitably replicated in technology, as they produce, on a large scale, prejudices and stereotypes that negatively affect the mediation between the human and the machine.¹⁵ Just as we humans are subject to heuristics and biases in our decision-making, the algorithms are too.¹⁶

Allied to this false idea of technology neutrality is the exponential growth in the ability to process personal data of the most diverse orders, precisely because of the advent of advanced artificial intelligence technologies, with the use of sophisticated algorithms and the possibility of machine learning. The treatment of “big data”—literally, large databases—through increasingly developed computational techniques can lead to probabilistic results that, while reaching the interests of a specific part of the population, take away the individual’s capacity for autonomy and their right of access to goods, services, public policies, for example.

In this sense, the principle of nondiscrimination (provided, for example, in Article 6, IX of the Brazilian General Data Protection Law) must be reflected in all circumstances in which the use of data, whether sensitive or not, generates some misjudgment or inducement to results that would be unfair. Accordingly, this principle should serve as a basis for sustaining the protection of sensitive data, especially when we are faced with exercising democracy and access to social rights, such as the right to work, health, and housing.

One of the practices with a high potential to cause discrimination is

14. ANGELE CHRISTIN ET AL., COURTS AND PREDICTIVE ALGORITHMS 1 (2015), https://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf.

15. See generally CATHY O’NEIL, WEAPONS OF MATH DESTRUCTION (2016); ELI PARISER, THE FILTER BUBBLE (2011); Camila Souza Arango, Wagner Meira Jr. & Virgilio Almeida, *Identifying Stereotypes in the Online Perception of Physical Attractiveness*, in 1 SOCIAL INFORMATICS 419 (Emma Spiro & Yong-Yeol Ahn eds., 2016); Aylin Slam-Caliskan, Joanna J. Bryson & Arvind Narayanan, *Semantics Derived Automatically from Corporate Language Necessarily Contain Human Biases*, 356 SCIENCE, 183-86 (2017); Joy Buolamwini, *How I’m Fighting Bias in Algorithms*, TED (last visited August 8, 2022), https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms.

16. See generally PLOUS SCOTT, THE PSYCHOLOGY OF JUDGEMENT AND DECISION MAKING (1993) (discussing the influence of heuristics on human decision-making).

profiling, where the controller creates the data subject's profile, which is intended to serve as an evaluation parameter on some aspects of the subject's personality. In this scenario, it is evident there is a need for forms of controlling these practices to avoid and even mitigate risks of potential discrimination, illegality, or abuse in processing personal data.

From this perspective, when faced with the processing of data that makes use of algorithmic probability and machine-learning models for decision-making, indeed what is in dispute, depending on the legal interest involved in the decision, is whether the data controller will or will not be denying or even promoting the fruition of a fundamental right to data protection. Therefore, it will be essential to know if the process of decision-making was discriminatory concerning the data subject or a social group that the subject represents (people with disabilities, the elderly, and BIPOC, among others). This evaluation is necessary to verify that the result of applying the controller's algorithm not only refrains from committing this discrimination but also whether it fails to adequately promote the right to data protection.

Considering that these applications are increasingly having a substantial impact on sensitive social areas, such as the use of data providing for the development of humanitarian aid, accurate medical diagnosis, or rationality to decisions,¹⁷ these automated decisions may affect individual and collective rights (Article 5 of the Brazilian Federal Constitution) of data subjects, but also their social rights (Article 6 of the Brazilian Federal Constitution).

Furthermore, the principle of equality is identified as one of the axiological substrates of the general clause for the protection of the human person, foreseen as one of the foundations of the Democratic State of Law in Article 1, III of the Brazilian Federal Constitution. More than the right to equal treatment, respect for differences and unequal treatment are forms of materialization of the dignity of the human person. Observing the constitutional context, the legal protection of personal data in the Brazilian legal system is due to the need to preserve the principle of equality—and the consequent principle of noncompliance discrimination—to support eventual, existential vulnerabilities.

Considering that the collection of personal data and the creation of social profiles may lead to discrimination, data protection should be seen as “the protection of life choices against any form of public control and social stigma” (L. M. Friedman) and as “vindication of the

17. Danilo Doneda & Virgilio Almeida, *O que é a governança de algoritmos*, in *TECNOPOLÍTICAS DA VIGILÂNCIA: PERSPECTIVAS DA MARGEM* [SURVEILLANCE TECHNOLOGIES: PERSPECTIVES FROM THE MARGIN] 141, 143 (Fernanda Bruno et al. eds., 2019).

boundaries protecting each person’s right not to be simplified, objectified, and evaluated out of context” (J. Rosen).¹⁸ Therefore, it is concluded that personal data protection—as a result of the general clause of protection of the human person, the right to privacy, and the principle of equality—is an essential requirement for democratic exercise.

A. *FACIAL RECOGNITION AND REGULATION IN BRAZIL*

In 2018, the Brazilian General Data Protection Law (LGPD) was passed, aiming to protect the rights of holders of personal data and impose a series of obligations to be complied with by those who process data in the country. Despite not mentioning at any time the facial recognition technology or even AI systems as an object of regulation, the LGPD is the law applicable to situations where such technologies are used. The LGPD applies because these technologies use personal data to achieve the desired results. Whereas people’s images (specifically the face) are understood as biometric data, facial recognition systems meet the regulatory framework already established in the LGPD. In this sense, we can indicate some aspects of the LGPD that are guidelines for regulating facial recognition technology. The first concerns the principles applied to personal data processing activities (Article 6, LGPD). Here, we can consider three principles as being of direct relevance: the principle of prevention, which matters in the adoption of measures to prevent the occurrence of damages due to the treatment of personal data; nondiscrimination, which prohibits processing for unlawful discrimination; and responsibility and accountability, which requires the data processing agent to demonstrate the adoption of effective measures to comply with personal data protection rules.

Another relevant aspect of the LGPD is the recognition of the data subject’s right to request a review of decisions made solely based on automated processing of personal data that affects the person’s interests or aspects of the person’s personality (Article 20, LGPD). In addition, the data processing agent must provide clear information regarding the criteria and procedures used for the automated decision. Furthermore, LGPD recognizes the right of the Data Protection National Authority for carrying out an audit to verify discriminatory aspects in the automated processing of personal data.

On the other hand, a series of bills intended to regulate AI. In

18. Stefano Rodotà, *Data Protection as a Fundamental Right*, in REINVENTING DATA PROTECTION? 77, 78 (Serge Gutwirth et al. eds., 2009). See generally Stefano Rodotà, *Some Remarks on Surveillance Today*, 4 EUR. J.L. & TECH. (2013), <https://www.ejlt.org/index.php/ejlt/article/download/277/388?inline=1>.

Brazil, following what is happening in Europe, there is a specific bill, the PL 21/20, which is currently being debated in the federal senate. The bill establishes foundations, principles, and guidelines for developing and applying AI in Brazil. The project has received much attention, especially for its characteristic of being a principled and conceptual law, contributing little to the concrete regulation of situations in which AI is used.

However, two references must be made to the bill: (i) the inclusion of the security and prevention principle, which requires the person who provides the AI system to use technical, organizational, and administrative measures that allow the mitigation of risks from the operation of artificial intelligence systems, as well as (ii) the obligation imposed on public administration to implement concrete risk management, taking into account the definitions of the need for regulation of artificial intelligence systems and the appropriate level of intervention. The references to the management and mitigation of risks, considered beacons for the use of AI systems and the protection of fundamental rights, generate the obligation of a continuous assessment of AI uses and applications that require thoughtful analysis of the proportionality and adequacy in the use of such systems when opposed to the fundamental interests of the human person. It is precisely for this reason that we seek to assess whether the use of facial recognition systems—notably in applications used to provide public security and allow an “efficient” criminal prosecution—is proportionate and adequate to constitutionally guaranteed fundamental rights.

B. FACIAL RECOGNITION AND REGULATION IN EUROPE

Regulatory debates on AI and facial recognition technologies are already quite mature in Europe. In 2021, a bill was proposed, called the AI Act, which aims to ensure that Europeans can benefit from new technologies developed and functioning according to European Union values, fundamental rights, and principles.

The regulation follows a risk-based approach and differentiates between uses of AI that create: (a) an unacceptable risk, (b) a high risk, and (c) a low or minimal risk. In addition, the AI Act, in Title II, establishes a list of prohibited AI practices. The list includes all AI systems whose use is considered unacceptable for violating the values of the EU—for example, violating fundamental rights. The bans cover practices with significant potential to manipulate people through subliminal techniques that go unnoticed or explore the vulnerabilities of specific groups, such as children or people with disabilities, to materially distort their behaviour in a way that is likely to cause

psychological or physical harm to them or another person. Other manipulative practices or exploratory approaches that are made possible by AI systems and that affect adults can be covered by legislation on data protection, consumer protection, and digital services, which ensures that individuals are adequately informed and are free to decide not to be subject to profiling or other practices that may affect their behaviour. The proposal also prohibits social classification based on AI for general use by public authorities. Finally, the use of “real time” remote biometric identification systems (FRTs) is not permitted in spaces accessible to the public when the objective is to maintain public order. This practice is considered particularly intrusive on the rights and freedoms of the data subjects, as they can affect the private life of a large part of the population, give rise to a sense of constant mass surveillance, and indirectly deter the exercise of freedom of assembly and other fundamental rights.

Considering the high risk that the use of FRTs brings to the exercise of democratic rights, the European Data Protection Board (EDPB) has called for FRTs to be banned from use under the proposed EU AI Act. The EDPB considers AI-supported facial recognition systems categorizing individuals based on their biometrics into clusters according to ethnicity, gender, and political or sexual orientation as incompatible with the European Charter of Fundamental Rights. In addition, the EDPB considers that “processing of personal data in a law enforcement context would rely on a database populated by a collection of personal data on a mass scale and in an indiscriminate way, e.g., by ‘scraping’ photographs and facial pictures accessible online,”¹⁹ in particular those made available via social networks, would, as such, not meet the strict necessity requirement provided for by Union law.

On the other hand, there is another proposal for a moratorium that intends to be sent to the European Parliament to regulate the uses of AI in criminal law and its use by police and judicial authorities in criminal matters (2020/2016(INI)).²⁰ The parliament aims to regulate the uses of AI technologies, specifically, the FRT, which is already being used to search databases of crime suspects, in addition to carrying out forecasting (predictive policing and analysis of crime points) with behaviour detection tools. According to parliament, applications of AI

19. EUROPEAN DATA PROTECTION BOARD, GUIDELINES 05/2022 ON THE USE OF FACIAL RECOGNITION TECHNOLOGY IN THE AREA OF LAW ENFORCEMENT (2022), https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

20. Resolution of 6 October 2021 on Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters, EUR. PARL. DOC. A9-0232/2021 (2021).

technology to law enforcement can have varying degrees of reliability and accuracy that can impact fundamental rights and the dynamics of criminal justice systems.

According to that document, the European Data Protection Board and the European Data Protection Supervisor request a moratorium on the “the deployment of facial recognition systems for law enforcement purposes that have the function of identification, unless strictly used for the purposes of identification of victims of crime.”²¹ Such a motion aims to set a deadline within which the technical standards for the use of this technology must be examined with full respect for fundamental rights and must not lead to prejudice and discrimination that could hinder the exercise of democracy.

C. INITIATIVES FOR A REGULATION OF THE USE OF FACIAL RECOGNITION TECHNOLOGIES

Among the initiatives to regulate facial recognition technologies, some can already be put into practice. First, laws that protect personal data or declarations of fundamental rights bring moral postulates that are recognized as principles (i.e., transparency, accountability, equality, etc.). On the one hand, the recognition of these principles is paramount for the protection of fundamental rights; on the other hand, their low enforceability leaves something to be desired when delimiting the uses of technologies. Nevertheless, in the absence of a “hard law,” those ethical or moral postulates are welcome as a first effort to regulate the use of FRTs.

The first proposal concerns the so-called principle of necessity and data minimization that intends to limit the collection and storage of personal data to the essential minimum to achieve the purposes indicated in the processing of personal data. Moreover, as a result of the recognition of the principle of transparency and accountability, it is required of organizations that use personal data processing technology to establish clear rules on the purpose and legal bases for the processing of those data, that is, the purpose of their use. Consequently, the holder can reject its use if it is employed in an abusive or illegal manner. One way to implement the principle of accountability is precisely the definition of transparent rules for data sharing, informing the holder of personal data in advance of such procedures. It is also of paramount importance to limit the processing of biometrics data in a single database and ensure that security systems information is robust and follows standards established by the community, in addition to allowing

21. *Id.* at art. 27.

that external bodies audit databases and personal data processing operations.

However, when regulatory standards are not implemented, our society lives in a legislative vacuum that has allowed the increasingly invasive use of technologies of facial recognition.

II. PART II

In this part, we argue that some use of technologies and digital surveillance—especially facial recognition—can lead to violence and, eventually, death. To explain our approach, we rely on Achille Mbembe’s notion of necropolitics. Through our updated and novel interpretation of Mbembe’s insights, we hold that new necropolitical interventions are relying on the use of data to subjugate, discriminate, and, eventually, eliminate given individuals. We call this phenomenon data necropolitics. To unpack our argument, we will first briefly explain Achille Mbembe’s idea of necropolitics.

A. “THE POWER TO TAKE LIFE”

The insight that death and violence still play a relevant political role in governing given populations has fostered numerous academic debates. Since Foucault’s perspective on biopower, authors such as Giorgio Agamben, Roberto Esposito, Mike Hill, and Warren Montag have insisted, respectively, on how the “power to take life” is still pervasive in the exercise of sovereignty, modern science, and liberal economics.²² Achille Mbembe has radicalized these perspectives, since it would be possible to understand genocides, famines, refugee crises, civil war, and so on, under a common paradigm, namely, necropolitics. This idea refers to the “subjugation of life to the power of death.”²³ Indeed, following Mbembe, a different sort of “weapons are [now] deployed in the interest of maximum destruction of persons and the creation of *death-worlds*, new and unique forms of social existence in which vast populations are subjugated to conditions of life conferring upon them the status of *living-dead*.”²⁴

It is possible to detect in Mbembe’s scholarship that the making of these *death-worlds* is produced through the interplay of at least four

22. MIKE HILL & WARREN MONTAG, THE OTHER ADAM SMITH 235-342 (2014). *See generally* GIORGIO AGAMBEN, HOMO SACER: SOVEREIGN POWER AND BARE LIFE (Daniel Heller-Roazen trans., 1998). *See generally* ROBERTO ESPOSITO, BÍOS. BIOPOLITICS AND PHILOSOPHY (Timothy C. Campbell trans., 2008).

23. *Id.*

24. ACHILLE MBEMBE, NECROPOLITICS 92 (Steven Corcoran trans., 2019).

factors.²⁵

First, necropolitics relies on *necroeconomies*. Late capitalism and neoliberalism would have produced an excess of populations that could not be exploited anymore, and, as a consequence, require management through their constant exposure to dangers. The climate crisis, erosion of socioeconomic rights, and unstable working conditions would be the most illustrative examples of this necroeconomy.

Second, necropolitics implies the confinement of given populations in specific territories, namely, campsites. Mbembe holds that the camp-form (refugees, prisons, banlieues, suburbs, favelas) are now the dominant technique to govern undesirable populations.

Third, necropolitics keeps on expanding in societies thanks to racism. This can have different forms (institutional, systemic, subjective), and it enables discrimination and humiliation of “anyone considered not to be one of us.”²⁶

Fourth, necropolitics aims at producing “death on a large scale.”²⁷ State terror, wars, and predation of natural resources “manufacture an entire crowd of people who specifically live at the edge of life, or even on its outer edge—people for whom living means continually standing up to death . . .”²⁸

Mbembe’s necropolitics have been applied and discussed in numerous fields of academic research, such as the latest pandemic, the conditions of inmates, the conditions of asylum seekers, the marginalization of indigenous people, and the climate crisis.²⁹ It is only very recently that scholars have intended to examine the pervasiveness of death under our current “digital revolution.” Evelyn Wan refers to necropolitics to define the mining of minerals necessary to our digital

25. See Antonio Pele, *Achille Mbembe: Necropolitics*, CRITICAL LEGAL THINKING (March 2, 2020), <https://criticallegalthinking.com/2020/03/02/achille-mbembe-necropolitics/>.

26. MBEMBE, *supra* note 24, at 54.

27. *Id.* at 37.

28. *Id.*

29. See Bárbara L. C. V. Dias & Jean-François Y. Deluchey, *The “Total Continuous War” and the COVID-19 Pandemic: Neoliberal Governmentality, Disposable Bodies and Protected Lives, Law, Culture and the Humanities*, L., CULTURE & HUMANITIES 4–5 (2020); Frédéric Le Marcis, *Life in a Space of Necropolitics*, 84 ETHNOS 74, 74–77, (2019); Ariadna Estévez, *The Politics of Death and Asylum Discourse: Constituting Migration Biopolitics from the Periphery*, 39 ALTS. 75, 77 (2014); Carl Death, *Africanfuturist Socio-Climatic Imaginaries and Nnedi Okorafor’s Wild Necropolitics*, 54 ANTIPODE 240, 240–42, 245–46, 250–52, 254–55 (2022). See generally Sophia Martensen, *Necropolitics, Colonialism, and Indigenous Peoples in Canada*, 3 YORK UNIVERSITY CRIMINOLOGICAL REV. (2021).

infrastructure.³⁰ Vural Ozdemir et al. have explored how “digital death and grieving” are becoming commodities of digital culture.³¹ Francesca Maria Romeo refers to “digital necropolitics” to examine “how images of the dead and the dying circulate within various digital contexts”³²

Our discussion on data necropolitics intersects these debates and is also more ambitious since we argue that the current production and exploitation of digital data can produce a novel production of death targeting growing, vulnerable populations. Mbembe holds that necropolitics can be twofold. It is “*the generalized instrumentalization of human existence and the material destruction of human bodies and populations.*”³³ Under this perspective, necropolitics implies, on the one hand, exploiting and consuming human lives through socioeconomic exploitation, and, on the other, destroying human existences through the lack of access to basic rights, or even physical elimination.

In this part, we hold that data necropolitics oscillates between these two dimensions. First, data can produce and normalize the vulnerabilities that given populations have been facing (i.e., racial bias). Second, it can legitimize and turn invisible the violence and death those same populations have been suffering. Violence should not be understood as “mere” physical aggression or violation of private property rights. It is also socioeconomic and symbolic. When we refer to data necropolitics, we have in mind not only the physical elimination of certain individuals but also a predatory/digital form of governance that exposes and produces social violence, vulnerability, and, eventually, (social) death. It circulates below and sets the foundations of our technological welfare. We will examine different fields where data necropolitics can be deployed. First, we will examine how facial recognition in Latin America and Brazil, in particular, can be understood within a data-necropolitical framework since it relies on legal vacuums and targets vulnerable populations. Second, we will interpret specific military and intelligence activities (i.e., drones) as other forms of data necropolitics. Finally, regarding health inequalities, we will understand how data necropolitics can work not only through an excess of data but also a (voluntary) lack of data concerning a given

30. Evelyn Wan, *Labour, Mining, Dispossession: On the Performance of Earth and the Necropolitics of Digital Culture*, 15 INT’L J. PERFORMANCE ARTS & DIGIT. MEDIA 249, 251–52 (2019).

31. Vural Özdemir et al., *Thanatechnology and the Living Dead: New Concepts in Digital Transformation and Human-Computer Interaction*, 25 OMICS 401, 402, 404 (2021).

32. Francesca Maria Romeo, *Towards a Theory of Digital Necropolitics* 7 (June 2021) (Ph.D. dissertation, University of California, Santa Cruz), <https://escholarship.org/uc/item/1059d63h>.

33. MBEMBE, *supra* note 24, at 68.

population.

B. FACIAL DATA NECROPOLITICS

According to Mbembe, necropolitics relies on “[i]nsidious techniques of mass surveillance” that create “a segmented planet of multiple speeds” where the basic (digital) rights of vulnerable populations are bluntly ignored.³⁴

Facial recognition has slowly but surely been deployed in Latin America, and this example shows the prescient insights of Mbembe. The use of facial recognition in Latin America has been mostly implemented “without any kind of public consultation” and thanks to “deficient regulatory context[s],” according to the latest report of AlSur, a consortium of eleven civil society and academic organizations from Latin America.³⁵ Regarding the areas of application of facial recognition, public security and surveillance of public spaces are the most relevant.³⁶ It is also worth mentioning other areas, such as transportation, social care, and health.

In Brazil, three examples of facial recognition deployment can illustrate these trends: transportation, public security, and health care. Since 2018, the metro of São Paulo has been gathering data—through facial recognition—without the consent of its users. It was only in 2021 when the systems were deactivated, thanks to court orders (ViaQuatro and Edital de Licitação do Metrô de São Paulo).

As a second example, twenty Brazilian cities have been experimenting with facial recognition for law enforcement purposes. Brazil’s federal public authorities have designed a pilot project (Em Frente Brasil) providing, since 2019, specific public funding to cities interested in this initiative. This project relies on partnerships with foreign tech companies (mostly from China, Europe, and Israel) that have offered their surveillance equipment to this public program.³⁷

Finally, the discreet but sustained deployment of facial recognition in Brazil appears in the intriguing case of the Brazilian NGO, the Central Única das Favelas (CUFA). For more than twenty years, this NGO has promoted art, education, sport, music, and leisure among Brazil’s vulnerable youth communities. Like many other NGOs, CUFA launched an initiative to distribute free food baskets in the favelas

34. *Id.* at 50, 101.

35. ALSUR, FACIAL RECOGNITION IN LATIN AMERICA: TRENDS IN THE IMPLEMENTATION OF A PERVERSE TECHNOLOGY 7, 8 (2021).

36. *Id.* at 7.

37. Jonas Valente, *Face Recognition Tech Gains Ground in Brazil*, AGÊNCIA BRASIL (Sept. 20, 2019, 2:14 PM), <https://bit.ly/3KKXrOf>.

during the COVID-19 pandemic. However, in contrast to other similar initiatives, CUFA also planned to use facial recognition to register the potential two million beneficiaries. A partner tech company offered its expertise to collect all the biometric data. Amid critiques raised by activists and scholars regarding the final use of the collected data, CUFA decided to give up the use of facial recognition.³⁸

Those cases reveal how AI and facial recognition still rely on and produce racial bias and criminalize Afro-Brazilian and other Brazilian vulnerable populations. The cases also show the lack of transparency in the collection and storage of data.

Despite the relevance of these questions, another issue should be addressed. The lack of efficient national regulation and legal vacuums regarding the precise use of facial recognition is designed to foster the deployment of these technologies. In other words, data necropolitics, namely, the circulation of predatory and digital forms of power, depends on a deficient regulatory framework to gather data from vulnerable populations.

While the Global North, as we have seen above, has adopted relatively strong regulations regarding facial recognition and AI, like the upcoming EU regulation on AI, these technologies are being tested in Latin America and in the Global South in areas that are forbidden in the Global North. It is also with the help of companies situated in Europe, China, Israel, and the United States that data necropolitics can be performed. So far, as we have seen above with Brazil, these technologies are deployed in areas such as transportation, public security areas, and public health. Data necropolitics penetrates precisely into the breach of the social and institutional weakness of the Global South, namely, criminality/violence and socioeconomic inequalities. It is at this intersection where data necropolitics is the most predatory since it targets the most vulnerable populations of the world. Here, data necropolitics is disguised by what we call “techno philanthropic capitalism.” Technological donations and trial run technological experiments aim at filling the social and economic vacuum of many Latin American and Global South societies. Some tech companies intend to consolidate their foothold, building a strong relationship with officials while massively collecting data from citizens to improve their technologies.³⁹ It is not only the violent data extraction

38. Alessandro Feitosa Jr., *Por que a Cufa interrompeu o uso de reconhecimento facial após polêmica* [Why Cufa Stopped Using Facial Recognition after Controversy], *G1* (Apr. 27, 2021, 8:17 PM), <http://glo.bo/3KlcYOW>.

39. Leo Schwartz, *Major Surveillance Firms are ‘Gifting’ Tools to Find a Foothold in Latin America*, *REST OF THE WORLD* (Aug. 12, 2021), <https://bit.ly/3q7COlQ>.

of “data colonialism,”⁴⁰ but also, foremost, a seeming techno-philanthropic ethos that pretends to fix state failures and help vulnerable communities.

These ongoing strategies turn the Global South and Latin America into giant and open laboratories for the experimentations of AI, facial recognition, and mass data surveillance. Because of legal weakness and political complacency, these populations are becoming the digital guinea pigs of data necropolitics. Facial recognition (and other technologies) are indeed insidious techniques that segment the planet into different populations that can be, more or less, observed and manipulated.

The effectiveness and the lack of a legal regulatory framework play a relevant role in the deployment of this predatory form of data necropolitics. Brinks, Levitsky, and Murillo have presented a comprehensive approach to *The Politics of Institutional Weakness in Latin America*, bringing to light “limited enforcement, insufficient state capacity, or societal cooperation.”⁴¹ Among the roots of “institutional weakness” in this region, the authors have underlined socioeconomic inequality, low state capacity, and economic/political volatility.

“Thus, much of Latin America may be suffering from a self-reinforcing cycle in which social inequality and economic and political instability generate institutional weakness, which, in turn, reinforces inequality and instability.”⁴² It is possible to add that data necropolitics relies on Latin America’s institutional weakness, a process that would ultimately bring about more inequalities and suffering among the vast majority of the Latin American population.

After having examined facial recognition in Latin America through data necropolitical lenses, we will explore, in the following part, the functions of the drone and mass surveillance.

C. ON DRONES AND DIGITAL SURVEILLANCE

“By creating new military markets, war and terror have transformed into modes of production, period.”⁴³ Necropolitics is, therefore, entrenched in late capitalism and neoliberalism. From Mbembe’s interpretation, it is possible to unfold how data economy is also related to necropolitics and wars.

40. See generally Nick Couldry & Ulises A. Mejias, *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*, (2019) (defining “data colonialism” and detailing how it is used in the current era of pervasive datafication).

41. DANIEL M. BRINKS ET AL., *THE POLITICS OF INSTITUTIONAL WEAKNESS IN LATIN AMERICA* (2020).

42. *Id.* at 291.

43. MBEMBE, *supra* note 24, at 36.

The more prominent roots of data necropolitics are related to military activities and intelligence activities. The relationships between the military industries, intelligence services, and big tech are even more critical. The current global race on AI supremacy and the economic stakes underpinning data surveillance show those core political issues.

The Pentagon’s Project Maven is currently involving Silicon Valley companies, such as Google, to boost and apply AI technologies in the defence project.⁴⁴ The UK intelligence services have recently signed a contract with Amazon to store sensitive data in the cloud of the US-based firm.⁴⁵ A similar agreement was signed in 2015 between the French intelligence services and the US-based firm Palantir.⁴⁶ Also, two French tech companies have been charged with complicity in torture for selling surveillance equipment to Libya and Egypt.⁴⁷

These examples certainly reveal the competition (and collaboration) between tech companies to access profitable public contracts. Regarding the issue of this paper, these examples show how a myriad of public and private actors are collaborating (and competing) “to produce total information, the first and most important prong of counterinsurgency paradigm.”⁴⁸

Following the prescient analysis of Bernard E. Harcourt, the counterinsurgency strategies (once used in the battlefields in colonial settings and after 9/11) are now a model of national governance in most countries. Counterinsurgency tactics with the deployment of massive surveillance programs and hyper-militarized policing are now deployed against groups that are not active insurgent minorities, namely, asylum seekers, refugees, Muslims, Afro-American protesters, eco-activists, etc. Harcourt mentions three main counterinsurgency strategies: first, to collect all data and achieve total awareness; second, to eradicate the active minority; and, finally, to gain the consent of the majority of the population.⁴⁹

It is possible to understand the increasing collaboration between

44. Tom Simonite, *Pentagon Will Expand AI Project Prompting Protests at Google*, WIRED (May 29, 2018, 7:00 AM), <https://www.wired.com/story/googles-contentious-pentagon-project-is-likely-to-expand>.

45. Helen Warrell and Nic Fildes, *Amazon Strikes Deal with UK Spy Agencies to Host Top-Secret Materials*, FINANCIAL TIMES (October 25, 2021), <https://on.ft.com/3Q6oyEH>.

46. Mathieu Rosemain, *A French Alternative to Palantir Would Take Two Years to Make, Thales CEO Says*, REUTERS (October 23, 2020, 1:34 PM), <https://reut.rs/3ReumNM>.

47. Sarah Elzas, *French Executives Face Torture Charges for Selling Spy Gear to Libya, Egypt*, RFI (June 22, 2021, 1:13 PM), <https://www.rfi.fr/en/france/20210622-french-executives-face-torture-charges-for-selling-spy-gear-to-libya-egypt-amesys-nexa-human-rights>.

48. BERNARD E. HARCOURT, *THE COUNTERREVOLUTION* (2018)

49. HARCOURT, *supra* note 48, at 13–14.

tech companies, intelligence services, and the military, under Harcourt's counterrevolution paradigm. Indeed, "the boundaries between counterinsurgency as foreign policy and counterinsurgency as domestic governance begin to crumble as more and more data is necessary for more effective data mining. As the battle against terror goes global, so do the populations to target—including our own."⁵⁰

As a consequence, counterrevolution produces an increasingly social, political, and digital vulnerability that targets the behaviour of given populations. Timnit Gebru and the DAIR Institute have revealed how AI can foster racism and may harm vulnerable groups.⁵¹ Shaka McGlotten advances the idea of "Black data" to grasp how Black people are marginalized by big data through race.⁵² There is a growing scholarship examining racial, ethnic, and socioeconomic bias in the digital world.⁵³ In any case, our notion of data necropolitics intersects Harcourt's concept of counterrevolution and both shape forms of governance that enhance the discriminations that vulnerable populations have been suffering.

One of the radical forms of data necropolitics, namely, the ability to kill remotely and automatically, is epitomized by drone strikes. "Death by data" shows the role of algorithms in targeted killings.⁵⁴ A 2021 report of the UN Panel of Experts on Libya suggests that in March 2020 the first attack launched automatically by an AI-based drone was registered.⁵⁵ While Western countries and China are massively investing in Lethal Autonomous Weapons Systems (LAWS), the UN has declared that their use should be prohibited by international law. However, powerful states refuse any sort of regulation since these new forms of weapons are becoming crucial to their respective and alleged

50. *Id.* at 66.

51. See *Research Philosophy*, DAIR INST., <https://www.dair-institute.org/research> (last visited Oct. 29, 2022).

52. Shaka McGlotten, *Black Data*, THE SCHOLAR AND FEMINIST ONLINE (Feb. 13, 2014), <https://sfoonline.barnard.edu/shaka-mcglotten-black-data>.

53. See generally LIZZIE O'SHEA, *FUTURE HISTORIES: WHAT ADA LOVELACE, TOM PAINE, AND THE PARIS COMMUNE CAN TEACH US ABOUT DIGITAL TECHNOLOGY* (2019); Greta Byrum & Ruha Benjamin, *Disrupting the Gospel of Tech Solutionism to Build Tech Justice*, STAN. SOC. INNOVATION REV. (June 6, 2022), https://ssir.org/articles/entry/disrupting_the_gospel_of_tech_solutionism_to_build_tech_justice; Stephen Kearse, *The Ghost in the Machine: How new technologies reproduce racial inequalities*, THE NATION (June 15, 2020), <https://www.thenation.com/article/culture/ruha-benjamin-race-after-technology-book-review>.

54. Jennifer Gibson, *Death by Data: Drones, Kill Lists and Algorithms*, E-INTERNATIONAL RELATIONS (Feb. 18, 2021), <https://www.e-ir.info/2021/02/18/death-by-data-drones-kill-lists-and-algorithms>.

55. Joe Hernandez, *A Military Drone with a Mind of its Own was Used in Combat*, U.N. SAYS, NPR (June 01, 2021, 3:09PM), <https://n.pr/3Q3BHym>.

national security.

Experts and activists have, therefore, warned against the non-prohibition of LAWS, since they would potentially trigger more violence. Indeed, in words that are tragically similar to Mbembe’s necropolitics, LAWS could “facilitate violence on a large scale.”⁵⁶ Additionally, “with facial recognition and other technologies, they can target individuals or groups . . . which could appeal to violent groups and state militaries committing political assassinations and ethnic cleansing.”⁵⁷ Finally, “LAWS may make it easier for those who control them to hide their identities.”⁵⁸

As Gregoire Chamayou presciently suggests in *A Theory of the Drone*, while ethics, in general, refers to the set of doctrines of living well and dying well, a “necroethics,” namely, the ability of “killing well,” is shaping our understanding of current and future wars.⁵⁹ The “necroethics of the drone [and LAWS] abandon[] any discussion of fundamental issue” since “the targets are presumed guilty until they are proved innocent—which, however, can only be done posthumously.”⁶⁰ Consequently, following Chamayou, “by ruling out the possibility of combat, the drone destroys the very possibility of any clear differentiation between combatants and noncombatants.”⁶¹

Simultaneously and more profoundly, the development of autonomous weapons has broader consequences for our societies. Indeed, it is worth reminding that “[t]he State’s dependence on the bodies of the lower classes to wage war was also one of the factors that made it possible for those classes to establish a durable bargaining of power.”⁶² In other words, the history of the welfare state is a result of warfare as Thomas Piketty and Michel Foucault have notoriously shown it under biopolitical lenses.⁶³ It is relevant to understand that under the deployment and logic of LAWS “the promise to preserve national lives goes hand in hand with the *increased social vulnerability and precariousness of many of those lives*.”⁶⁴ Therefore, with our notion of

56. Robert F. Trager, *Killer Robots Are Here—and We Need to Regulate Them*, FOREIGN POLICY (May 11, 2022, 1:46 PM), <https://foreignpolicy.com/2022/05/11/killer-robots-lethal-autonomous-weapons-systems-ukraine-libya-regulation>.

57. *Id.*

58. *Id.*

59. GRÉGOIRE CHAMAYOU, *A THEORY OF THE DRONE* 146 (Janet Lloyd, trans., 2015).

60. *Id.*

61. *Id.* at 147.

62. *Id.* at 193.

63. See THOMAS PIKETTY, *CAPITAL IN THE TWENTY-FIRST CENTURY* (Arthur Goldhammer, trans., 2017); MICHEL FOUCAULT, *THE BIRTH OF BIOPOLITICS* (Michael Senellart, ed., Graham Burchell, trans., 2010).

64. CHAMAYOU, *supra* note 59, at 194 (emphasis added).

data necropolitics, we can understand how the development of autonomous and AI-based weapons is entrenched on the socioeconomic pauperization of vulnerable communities.

It is not only the massive collection of data that might trigger discrimination and injustice but also the insufficient existence of data regarding given populations. Data necropolitics is entrenched not only to pervasive surveillance but also to a lack of data, namely, what we call a “digital or data gap.”

D. MISSING DATA AS NECROPOLITICS

Data necropolitics can operate not so much from an excess of data and surveillance on a given vulnerable population, but, on the contrary, through the absence or deficient use of data.

The COVID-19 pandemic has brought to light how the lack of data can enhance social and racial injustice. Regarding health inequalities during the pandemic in the United States, Rashida Richardson holds that “government data practices in the public health sector represents one extreme where insufficient collection, use, and reporting of ethnoracial health data can disguise underlying problems and tacit discrimination that aggravate and hasten racial inequities and harms including excess death.”⁶⁵ Similarly, in Brazil, the federal government tried to withdraw data concerning the pandemic’s daily infections and deaths.⁶⁶ Death by reporting date and epidemiological week were not published, just like the curve of new cases by reporting date and epidemiological week.⁶⁷

Also, the first epidemiological reports regarding COVID-19 did not take into account the racial impact of the virus, an approach that is legally compulsory in any official public health information in Brazil. Consequently, and just like in the United States, the mortality impact of the virus on black, brown, and indigenous populations was underreported.⁶⁸ In a prescient work regarding France’s management of the latest pandemic, Mathieu Arminjon and Régis Marion-Veyron have

65. Rashida Richardson, *Government Data Practices as Necropolitics and Racial Arithmetic*, GLOBAL DATA JUSTICE (Oct. 8, 2020), <https://globaldatajustice.org/gdj/1977/> (emphasis added).

66. Dom Phillips, *Brazil Stops Releasing Covid-19 Death Toll and Wipes Data from Official Site*, THE GUARDIAN (June 7, 2020, 1:40PM), <https://www.theguardian.com/world/2020/jun/07/brazil-stops-releasing-covid-19-death-toll-and-wipes-data-from-official-site>.

67. *News Organizations Team Up to Provide Transparency to Covid-19 Data*, O GLOBO (June 6, 2020) <http://glo.bo/3pZk2wZ>.

68. Márcia Pereira Alves dos Santos et al., *População negra e Covid-19: reflexões sobre racismo e saúde* [The Black Population and COVID-19: Reflections on Racism and Health], 34 ESTUDOS AVANÇADOS 225, 225–43 (2020).

highlighted the lack of data regarding social vulnerability to COVID-19 and more generally France’s myopia regarding biostatistics, becoming factors that have also normalized health injustice.⁶⁹

Data necropolitics evolved through data gaps, where data are insufficiently collected. This situation normalizes health injustice and, eventually, death. Didier Fassin’s scholarship has been exploring how health inequalities do not succeed by accident, but are the results of political and social choice. “Bio inequalities” shape different hierarchies of human lives.⁷⁰ The missing data and/or the deficient use of data regarding the morbidity of given populations in times of the pandemic have revealed and enhanced the moral and political hierarchies of individual lives regarding their racial and socioeconomic profiles.

CONCLUSION

Our paper has examined some potential risks unfolding from the nonregulation of specific uses of AI, facial recognition, and, more generally, digital data. Our approach has compared specific cases in the Global North and in the Global South. It has demonstrated the implementation of new technologies and their respect of basic rights, depending on legal and regulation frameworks. We have also shown how the lack of regulation can unfortunately lead to discrimination, injustice, and violence. Data necropolitics is a reality for many individuals belonging to vulnerable populations. It is therefore important to keep addressing these issues and bring forward public and private initiatives that keep on building the rule of law, the common good, and the respect of human rights.

69. Mathieu Arminjon & Régis Marion-Veyron, *Coronavirus biopolitics: the paradox of France’s Foucauldian heritage*, 43 HIST. AND PHIL. LIFE SCIS 1, 3 (2021), <https://link.springer.com/article/10.1007/s40656-020-00359-2>. Cf. Daniele Lorenzini, *Biopolitics in the Time of Coronavirus*, 47 CRITICAL INQUIRY 40, 40–45 (2021), <https://www.journals.uchicago.edu/doi/10.1086/711432> (explaining how the COVID-19 pandemic has revealed various ways society relies on systemic economic and racial inequalities); Antonio Pele & Stephen Riley, *For a Right to Health Beyond Biopolitics: The Politics of Pandemic and the Politics of Life*, L., CULTURE AND THE HUMANITIES 1 (2021), <https://doi.org/10.1177/1743872120978201> (discussing how prioritizing a human right to health can function as a shield against discrimination).

70. See Didier Fassin, *Another Politics of Life is Possible*, 26 THEORY, CULTURE & SOC’Y 44, 60–56); DIDIER FASSIN, LIFE: A CRITICAL USER’S MANUAL 66 (2018).

ACKNOWLEDGEMENTS

This work has been partly conducted under the European Union Marie Skłodowska-Curie Action “HuDig19,” Grant agreement ID: 101027394 led by Professor Antonio Pele (EHESS/IRIS, Paris & The Columbia Center for Contemporary Critical Thought, New-York)

The authors have no conflict of interest to disclose.