pensar
Revista de Ciências Jurídicas
e-ISSN: 2317-2150
Universidade de Fortaleza

The hiding of social harm in capitalist criminal surveillance and the anti-ethics of research in technological production[1]

A ocultação de danos sociais na vigilância penal capitalista e a antiética da pesquisa na produção tecnológica

Felipe da Veiga Dias*

Abstract:

The present study has as its theme social control in the current capitalist model and the social damage generated by corporate practices in the technological field. Based on this, the following question is structured: on the part of the technological-corporate production linked to the field of social control, is there a pattern based on ethical violations and the concealment of the social damage produced? The main objective is to determine if there is an unethical pattern that generates damage, as well as to understand which elements have been characterizing such violations, based on the criminological bias, on the part of the practices of technological corporations, which act directly in the improvement of social control. Methodologically, it starts from a deductive approach, in combination with the monographic procedure and the indirect documentation research technique. Finally, it is concluded that the constant disrespect of ethical bases in research and technoethics configure a corporate modus operandi, which increases the social damage caused to the population, and, in particular, when questionable technological devices are inserted in the penal system.

Keywords: penal control; social damages; surveillance capitalism; research ethics; technoetics.

Resumo:

O presente estudo tem como tema o controle social no atual modelo capitalista e os danos sociais gerados pelas práticas corporativas do campo tecnológico. Com base nisso estrutura-se o seguinte questionamento: há por parte da produção tecnológico-corporativa ligada ao campo do controle social um padrão baseado em violações éticas e na ocultação dos danos sociais produzidos? Traça-se como objetivo central determinar se há um padrão antiético gerador de danos, bem como compreender quais elementos vêm caracterizando tais violações, com base no viés criminológico, por parte das práticas das corporações tecnológicas, as quais atuam diretamente no aprimoramento do controle social. Metodologicamente parte-se de uma abordagem dedutiva, em combinação com o procedimento monográfico e a técnica de pesquisa da documentação indireta. Por fim, conclui-se que o desrespeito constante das bases éticas em pesquisa e da tecnoética configuram um modus operandi corporativo, o qual incrementa os danos sociais provocados à população e, em especial, quando da inserção de dispositivos tecnológicos questionáveis no sistema penal.

Palavras-chave*: controle penal; danos sociais; capitalismo de vigilância; ética em pesquisa; tecnoética.*

[1] Texto traduzido a partir de Inteligência Artificial.

* Pós-doutor em Ciências Criminais pela PUC/RS. Doutor em Direito pela Universidade de Santa Cruz do Sul (UNISC) com período de Doutorado Sanduíche na Universidad de Sevilla (Espanha). Professor do Programa de Pós-Graduação em Direito da Faculdade Meridional (IMED) – Mestrado. Professor do curso de Direito da Faculdade Meridional (IMED) – Passo Fundo – RS. Brasil. Coordenador do Grupo de Pesquisa "Criminologia, Violência e Sustentabilidade Social". Advogado. Passo Fundo – Rio Grande do Sul – Brasil. https://orcid.org/0000-0001-8603-054X

1 Introduction

This research takes as its thematic axis the ideas of social control, duly inserted in the capitalist economic context, together with the social damages derived from the contumacious practices of the business-technological field. The subject's proposal is presented as a dialogue between the legal-criminological visions of damages/violations, power relations and studies in technology, in order to align them on the critical plane, rescuing here the meaning given to it by Foucault's classic text (1978), that is, it is not intended to prescribe the directions of technological surveillance, but only to offer the challenge of criticism, resistance, the rejection of certain paths traveled by societies and their punitive sanctions.

This study is therefore based on two combined theoretical matrices, the first of which is power relations and the second is critical criminological bias, based on the adoption of its epistemological rupture. It is important to situate such assumptions, considering that, through their adoption, the reading of social control becomes broader than the simple appreciation of the punitive practices defined by the legal-criminal conception, comprising a range of diverse consequences; At the same time, power dynamics also allow the understanding of contextual phenomena in the operations of the subjects and the governing populations (governmentality), with special contemporary help from technological devices (forming, according to some approaches and due to the prominence of these tools, a kind of technopolitics).

The combination of these theoretical foundations aims to "make visible the practices of punishment and punitive power that insist on perpetually transforming themselves and preventing other forms of life" (Amaral, 2020, p. 38), which in this case translates into the special meaning of ethical-technological leaks in the production of criminal surveillance and in the production of social damage.

Based on the initial assumptions, the following question is adopted as a research problem: is there a pattern on the part of technological-corporate production linked to the field of social control based on ethical violations and the concealment of the social damage produced? In response to the question that mobilizes reflection, the main objective outlined is to determine whether there are repeated acts capable of affirming the standardized performance of violations, which would potentially produce social damage and would be supported by the lack of ethical respect for their formation and, consequently, achieve the improvement of social control by such instruments.

To carry out the aforementioned purposes, the deductive approach method is used, considering that in the first part of the study general concepts will be established and, subsequently, the unveiling of ethical-technological issues applied to the penal system is specifically deepened. In addition, the monographic procedure method helps to carry out, given the department of generalist conjugations and the elaboration of punctual-critical research on the subject, as well as the research technique of indirect documentation, with bibliographic emphasis.

2 Surveillance capitalism: the commodification of life in data and the expansion of social control

Based on the understanding of social damage as an object of study (Sarmiento *et al*., 2014), the insufficiency of criminological evaluations circumscribed to the definitions of lawfulness and illegality in the legal field is perceived, that is, there is a range of actions that produce massive harm to human and non-human beings that deliberately escape the definitions of crime in the field of social control. It is healthy to mention that some of the behaviors mentioned have already been the object of criminological critical thinking regarding the contributions of penal control to the capitalist model (Larrauri, 1992, p. 112), however, the epistemological rupture that is now taking place is willing to add the facets that are still little denounced and some of them resignified by technopolitical instruments (Lama; Sánchez-Laulhe, 2020).

Some of the assumptions evidenced by criminological-critical studies remain complete in the current reading, such as the functional character of criminal or harmful behaviors in capitalism (Taylor; Walton; Young, 2007, p. 242), which dismisses notions of these behaviors as dissonances or deviations from the "natural" order of this socio-economic model. This is affirmed in view of the fact that the denial of the structural factor of capitalism continues to be an immunizing logic, so that in the face of crises, such as the financial crisis of the early twenty-first century, "the strategy was then to blame the supposedly pathological individuals, those who 'abuse the system', and not the system itself" (Fischer, 2020, p. 116).

Lazzarato (2013, p. 133) affirms, in a complementary sense, when assessing that the bailout of banking institutions and other bases of the current capitalist model in the financial crisis are not mere aids to economic maintenance. According to the author, such "ransoms" are, in reality, the promotion of a system and strategy of domination/imprisonment for debts

(kidnapping of the future that conditions behaviors) and that, in the event of collapse, the exploited will be charged the bill for the losses.

It is also worth noting that the neoliberal rationality/*ethos* (with its entrepreneur of the self) (Chignola, 2020, p. 51) dominant in current ways of life helps to accept the discourse of individual responsibility of common subjects/criminals/deviants/abusers of the system, hiding the disarticulation of social ties or the perception of macrostructural aspects. There is a kind of ethical-individual simplification for concealment purposes, with the additive "the reduction of social life to the mathematical conclusions of financial algorithms", instilling that if society does not see such a perspective as positive, it is because it would require its own reform (Berardi, 2020, p. 31).

Despite the continuity of characteristics (competitive production, increased profits, productivity, growth) (Zuboff, 2019, p. 68), capitalism stands out for its adaptive mutability. In this sense, the power relations developed with technological support provide a State-market cooperation that governs in favor of a new capitalism (Foucault, 2008. p. 127), which is based (significantly) on the productive freedom of data/metadata for the improvement of control. "Therefore, the so-called trade in data, metadata or information in general begins to move the interest of statecraft, regardless of the agent – public or private – that seeks such realization" (Dias, 2021b, p. 108).

The proposals that seek to understand the new stage of capitalism in its technological interconnection are diverse, related to topics such as the *Big data* (Brayne, 2021, p. 12) or digital platforms (Srnicek, 2017), which are extremely contributory to the evidence of nuances of data exploitation in the market or also to the functionalization of new agents to intervene in productive relations. Despite acknowledging the contribution of this type of analysis, this study emphasizes the conception of Zuboff (2019), who defines the current model as surveillance capitalism.

The surveillance model operationalizes the use of human experiences as raw material, translating these processes into behavioral data (Ruiz, 2021, p. 14), which serve to improve economic and social activities and at the same time generate a large surplus of behavior. This additional content feeds algorithmic systems with machine learning that seek to predict the actions of target subjects, formatting the prediction products, and "these prediction products are traded in a new type of behavioral prediction market" that Zuboff (2019, p. 14 – 15) calls "behavioral futures markets."

It is understood that the data-based capitalist economy aims at predictability as conditioning or automation of subjectivities, making use of productive stimulus in a "free" environment (duly directed freedom) for the multiple dynamics of exploitation and, consequently, of control-surveillance.

Just for the record, another link that again refers to part of neoliberal reasoning is the assumption of the absence of alternatives (Brown, 2019, p. 78 – 79), but duly applied to the corporate-technological field, more precisely by transmitting the idea that the decisions made are inevitable consequences of technology and not as an intentional part of market exploitation. An example of this mention is the indefinite storage of data, which is an economic decision and not an inevitable effect of technology (Zuboff, 2019, p. 21).

Thus, we have a capitalism that adopts companies as customers, with users being mere sources of raw materials (not to be confused with popular notions that these would be products) (Zuboff, 2019, p. 71). These individuals (reduced to the condition of data, divisible, compatible) (Deleuze, 2013, p. 226) producers of raw material (data/metadata) find themselves duly disarticulated in their machinic servitude/slavery, which tears them apart: "the components of their subjectivity (intelligence, affects, sensations, cognition, memory, physical force) are no longer unified in an 'I', they no longer have an individualized subject as a referent" (Lazzarato, 2014, p. 27).

However, the transformations go beyond users, and one of the first nuances of the surveillance model becomes more noticeable in its distinction from the old Fordist model. While the latter focused on the expansion of production, the former focuses on its differential: the ever-expanding behavioral extraction.

> It is important to point out the vital differences for capitalism in these two moments of originality at Ford and Google. Ford's inventions revolutionized production. Google's inventions revolutionized extraction and established the first economic imperative of surveillance capitalism: the extraction imperative. The imperative of extraction meant that the supply of raw materials had to be obtained on an ever-increasing scale. Industrial capitalism will require economies of scale to achieve a high rate of combined productivity at a low unit cost. In contrast, surveillance capitalism requires economies of scale to extract surplus behavior. (Zuboff, 2019, p. 87).

This characteristic highlights the reason why technopolitical dynamics operate in favor of stimulating the production of data or information about the subjects themselves, who understand such behaviors (demonstrations on social networks, access to media portals etc.) as an exercise of their freedom, without observing that their acts produce value in the extractivist logic of companies linked to the technological field shaping their own subjectivities (Chignola,

2015, p. 14). Just as a mention, it is worth mentioning that the constant demand (pressuring the self-promotional exposure of each person) for the absorption of data reaches the point of modifying basic physiological functions such as sleep, so that people rest superficially (affecting their health, which already seems to be a kind of social damage), configuring something similar to electronic devices with the *Sleep* (Crary, 2016, p. 22).

Another observation concerns the cult of the visionary that surrounds this market, in which variation in the activities of companies referred to as *Big tech companies*, such as Alphabet/Google, Meta/Facebook, Apple, Amazon, their directors/CEOs or their creative groups that make up the "vision" of the company, when in reality they are only strategies for the same objective, to increase the capture/extraction of behavioral surpluses capable of providing high amounts of business profitability (Zuboff, 2019, p. 127).

The aforementioned allusion is consistent with Morozov's (2018, p. 29) explanation, in the sense of pointing out discursive and terminological issues raised in debates in the technological field as a way of immunizing criticism or the real intentions of some of its practices. The author clarifies by indicating that few would oppose more information or technology, since it is linked to these elements to knowledge and progress. This discursive stance prevents the perception that content of a political or economic nature is directly associated with such technological mechanisms, since what could "break" the internet (a recurrent discourse when legal restrictions on corporate-technological activities are proposed), with legislation or restriction on data handling (avoiding harm to the population), would also affect the *Big tech companies* and their economies of data accumulation, storage and trade, thus preventing a very particular vision of "progress".

In addition, the naturalization of surveillance/control contained in terms, discourses, texts, subtexts and other productions that encompass new technologies is added. "The culture of surveillance is so introjected into our daily lives that we are not intimidated by using such police vocabulary as 'follow' and 'be followed' on social networks" (Beiguelman, 2021, p. 62).

Another relevant distinction of surveillance capitalism is with respect to monopolies, since as a rule they would be refuted for disfiguring private relations by "unjustly eliminating competition to raise prices at will. However, under surveillance capitalism, many of the practices defined as monopolistic actually function as a means of corralling the user-derived supply of raw materials" (Zuboff, 2019, p. 131).

Source hoarding is not focused on economic oppression (price increases or product protection), but on reserving the obtaining of raw material (data/behaviors) in the extraction of

each individual. Thus, technology companies are accused of a different type of monopolistic practices, since they want to mold humanity, reaching the maximum level of human-machine combination, duly automated (Foer, 2018, p. 12).

It is feasible to infer that the changes in capitalism mentioned above offer a different vision of the practices of control and surveillance of populations, since the dimensions of the potential damage are not reduced to mere nuisances of a connection of *Call Center* or a breach of privacy. This means that in surveillance capitalism the cost of implementing many of the "innovative" technologies and corporate practices that generate devices capable of monitoring, exploiting, controlling, and sometimes punishing parts of the population (Harcourt, 2015, p. 14).

The basic objective of surveillance is its capitalist purpose, more precisely to serve the markets of advertising, targeted sales or security (Schneier, 2015, p. 39). In this line of thought, the cooperation/collusion between the State and companies denounced by critical criminological thinking with respect to behaviors that produce massive social damage (Budó, 2016) is recalled, to resume the reasoning that the abuses perpetrated in the video surveillance market are intentionally ignored by the legal-criminal provisions. For this reason, Bridle (2019, p. 206) adds: "global hypervigilance depends on political secrecy and technological opacity, and one feeds on the other", and complements by denouncing that "surveillance is done because it can, not because it is efficient; And like other automation practices, because it shifts the burden of responsibility and blame to the machine."

Therefore, there would be concern about techno-vigilant expansion even if these processes served only the lucrative desires of this new capitalism, due to the production of harm to human beings or the environment (see the construction of the technological rhetoric of clouds as natural-immaterial objects, in order to mask the environmental costs in order to maintain their physical structures permanently) (Beiguelman, 2021, p. 69). However, when the logics of the data market and technological creation are transferred to the management of state-criminal control, another level of abuse/damage is reached. It is worth mentioning that this process of technological circulation between areas other than the initial incursions is also verified, and some spaces are understood as laboratories or tests for its improvement (O'Neil, 2017, p. 16), that is, the mechanism that extracts facial data for social networks can easily be transformed into a facial recognition device.

Evidence has already been documented that surveillance capitalism and its devices, when incorporated into the orbit of public security and the legal-criminal field, are capable of

generating significant losses, reiterating a new chapter of self-fulfilling prophecies (Zaffaroni, 2001, p. 129) against the same publics selectively defined by state punishment. In short, situations that would previously be challenged in legal-criminal proceedings, due to the damage caused by relating data in an unfair way and violating rights, end up being hidden through false objectivity, neutrality (Morozov, 2013, p. 184) or even legal protections (commercial contract secrets, intellectual property, copyright) of certain technological mechanisms, functioning as true black boxes (Pasquale, 2015, p. 8) that prevent its questioning (O'Neil, 2017, p. 15-16).

At this point, it is essential to refer to the work of O'Neil (2017, p. 15) on some algorithm models[2], essential for the data surveillance market, which only serve to technologically hide the discriminations and inequalities produced by society and the criminal justice system, as exposed by the tools for calculating the risk of recidivism, police and penitentiary.

In addition, the biases contained in technological instruments have already been denounced by a considerable part of critical scholars, citing research such as Noble (2018. p. 11 – 16), Sumpter (2019), Brayne (2021. p. 16), Beiguelman (2021), Amaral, Martins, and Elesbão (2021). Recent research shows that surveillance capitalism expands the collection of data/information for economic purposes and for the continuity of the persecution of the same subjects subject to social control, while at the same time expanding its network of observation/surveillance over more people (creating new niches of discrimination and technological persecution).

Therefore, the insertion of questionable technological devices in a penal system recognized for its selective action, reinforcing inequalities and social discrimination, constitutes an act of state irresponsibility and the absence of minimum protection of rights. However, in addition to the obviousness of the expansion of massive damage to the portions of the population that are subject to the usual persecution of criminal control, there is still one more component in this equation: the creation of several of these surveillance instruments originates from the violation of ethical requirements in research and the lack of knowledge of technoethics.

Therefore, in the next stage of this study, one more element is added to the critical reading of control and technology, more precisely the consideration of the ethical bulwarks that guide scientific production. Thus, it is intended to analyze whether technological innovations respect the parameters imposed on all fields of knowledge production, or if abuses/damages end up

[2] Algorithms can be understood as a "finite list of defined instructions for calculating a function, a step-by-step directive that allows automated processing, or reasoning that commands the machine to produce a certain output."*exit* of a certain entry/*entrance* (Dijck, 2016, p. 57).

being made invisible in the name of "progress/evolution", making their inclusion in the spheres of criminal control even more dangerous.

3 The lack of ethics in corporate-technological research and the naturalization of the violating practices of big tech

After the establishment of the operation of the current data and surveillance market, the focus is on determining compliance with the ethical bases by technological production, which translates into subsequent instruments of the penal system and, therefore, deserves the concern of the criminological-legal field.

In Brazil, when research involves human beings, it is not evaluated by a Research Ethics Committee (CEP), which evaluates, through multidisciplinary and transdisciplinary committees, the ethical guidelines of the study and issues opinions on the proposal. This system is coordinated by the National Commission for Research Ethics (CONEP) linked to the Ministry of Health, and due to its evaluation, it assumes part of the responsibility for interventions with human beings, either through the management of data, biological materials, or participant information (Brasil, 2021).

The basic system uses the Brazil Platform as a place of presentation to committees scattered throughout the country, and the analysis and approval of the project must be prior to the start of the study activities, that is, without the opinion of the Committee the project would be violating ethical and legal standards.

In this sense, there are several ethical guidelines, however, some of them are better known by researchers, such as Resolutions 466 and 510, and are also complemented by Circulars (as happened in relation to online studies in 2021 – Circular 01/2021). In the case of the former, it functions as a nucleus for structuring studies with human beings, defining what a research should present, such as: benefits and risks derived from it, the right to compensation or even assistance against damages (Brasil, 2012). While in the second, specific aspects of studies in social sciences and humanities are clarified that can dispense with the Committee's evaluations (situation of opinion polls, for example) and other details specific to the field (Brasil, 2016).

With the point of support in the reading of the aforementioned regulations, what remains, of course, is that one of the basic elements for such practices is the Informed Consent Form (TCF), which ratifies the will of the person, or their legal representative, to participate in the study without said consent being obtained with any type of defect. fraud or violence. thus

being aware of the implications of their participation. Thus, Resolution 466/2012 is categorical in requiring that all research involving human subjects, in any area of knowledge, must "obtain the free and informed consent of the research participant and/or his or her legal representative, even in the case of research that, by its nature, justifiably implies subsequent consent" (Brasil, 2012, p. 4).

One could still infer the community and social character to be objectified in these investigations, since the disposition of individuals voluntarily imposes some kind of collective benefit, at least that is how the resolutions guide. A relevant observation is that the required term requires clarity in language and communication with the people who are willing to participate in the research (Brasil, 2012, p. 5), i.e., the common practice of technology companies, commonly seen in applications, of intentionally listing confusing or lengthy terms of use, in addition to attacking legal norms in the field of consumer or contract law, It also prevents consent according to ethical guidelines.

However, technology corporations tend to produce justifications (supported by a degree of immunization typical of the criminality of the powerful) (Barak, 2015, p. 105; Budó, 2016, p. 128) for a true inversion of the ethical order of research, not to say simply rape. This is affirmed by conducting their "studies", which first of all test functions, devices or improvements of technologies under false pretenses in the population, without informing the appropriate purpose, providing information and without any allusion to the informed consent of the "participants", and then announcing their benefits-results, reminding, also, without assuming the unethical tests of involuntary guinea pigs.

The point of issue is that the experiments are aimed at the economic well-being of these companies (this means maximizing profits related to surveillance capitalism at work), without any agreement or justification to the users of some of these technological instruments.

The conduct of "research" such as those mentioned above can be seen in the experiment conducted by Facebook and Cornell University in 2014 on the online dissemination of emotions. In this case, adjustments were made to the main pages of the users of the social network (*feed*), and a kind of reinforcement of emotions was found, that is, those exposed to more content seen as "positive" acted/commented in this sense and the same happened with "negative" content (Kucharski, 2020, p. 174).

While it is quite evident that experiences linked to emotions are the preferred target of these platforms, since their algorithms perceive the predilection driven by the viscerality of these feelings (and, consequently, the production of data necessary for their capitalist model)

(Dijck, 2016, p. 32), there have been scientific manifestations and journalistic coverage that point to the ethical violation of manipulating users without consent. Even if the study was methodologically justified, to avoid responses conditioned by prior consent, because "when researchers deceive participants to obtain a natural reaction, they often inform them after the study" (Kucharski, 2020, p. 175), as is the case in the provision of resolution 466/2012 when referring to subsequent justified consent (Brasil, 2012, p. 4).

Despite the legal (because basic fundamental and human rights are violated, even before the inclusion of the recent constitutional provision for the protection of personal data in 2021) and ethical norms, no user received consent contact (ICF) before or after the experiment, i.e., the corporate-technological behavior is that such rules do not apply to their "innovations".

This situation is aggravated when part of this action is aimed at increasing punitive tools and criminal surveillance practices against the population. This is alluded to because a considerable portion of surveillance capitalism is in the combination between companies and States for mutual benefit, so large corporations such as Google, Apple, Facebook, Amazon, among others, "are destroying the principles that protect individuality" (Foer, 2018, p. 12) in favor of the creation of new monitoring and surveillance technologies aimed at public security and the penal system. even aware of their "mistakes", insufficiencies or conditioning.

The debate about the levels of surveillance, data collection and violations of rights (such as privacy) or ethical standards is demonstrated by Véliz from the act of waking up in the morning. Therefore, the first access to the phone during the day marks the first data point obtained, informing companies and apps about the times when the individual usually starts their activities and even who they were sleeping with, since the location of another nearby device can easily indicate this fact. As for the invasive nature of these practices in privacy and in the management of life in society, the exemplification is reinforced by being projected onto "smart watches", which can absorb data even before waking up or even sexual activities carried out in bed (Véliz, 2020, p. 8).

In addition, the author also comments that Amazon has a patent to use facial recognition on doorbells, in order to mark objects of interest. However, the police authorities have been demanding the use of private cameras in their activities, so such records of companies such as Amazon and Google could remain in the hands of the social control system, without any type of consent, consent or notice (Véliz, 2020, p. 8).

In a similar sense is the desire of public security agents to specify the location of people through cell phones (GPS), in order to determine the previous and subsequent actions of suspects, defendants, victims, and others involved (Schneier, 2015, p. 7).

That said, various applications and instruments would lend themselves to cooperation articulated with surveillance practices, given their obtaining of relevant content such as faces, biometrics, retina, location, etc., which are already ordinary acts in the use of *smartphones* (see unlocking by some of these means), or are even popular in the fevers of users, as in the case of Faceapp or TikTok. In this sense, there would be a clear deviation from the purposes that associated people with these mechanisms, thus composing a more unethical step for the dubious or fraudulent use of data and personal information.

> The problem of presentation and profiling by search engines extends to social networks or content-sharing platforms; This is all the more serious because the nature and quantity of the data collected, as well as the use of those data, take place, to a large extent, without the explicit consent of the users. Those who would have liked to deepen their knowledge in this regard generally find themselves with the opacity of a "black box", whose operation is protected by industrial secrets and intellectual property. (Loveluck, 2018, p. 247 – 248).

Surveillance associations and diversions carried out by private entities for cooperation in surveillance matters would already be in themselves motivating attention, but this aspect is aggravated by actions based on the ideal of predictability, whether in the police or with facial recognition devices, which have been defended in their application in the penal system. with a point of support in a supposed neutrality and objectivity, despite the fact that there are studies that demonstrate injustices, discrimination, and failures in their actions (Morozov, 2013. p. 184). Therefore, the preventive action of algorithms and AIs in the criminal field has been producing a series of violations of rights, social damages, in addition to affecting ethical aspects of the acts and their existential political connection. This last mention is confirmed by impediments to participation in protests (people were prevented from taking buses to the places based on the risk prediction offered by the algorithm – considering the subjects as "dangerous") or even public safety actions that anticipate behaviors, as is already the case in the US and other European countries (Amoore, 2020, p. 5), and which to some extent has been foreseen in certain test events in Brazil (Elesbão; Saints; Medina, 2020).

In this way, it is verified that the attention paid to algorithms, AIs and other technological innovations is justified in different critical planes, in which legal, criminological and ethical spaces are communicated. Another evidence of the violating pattern that naturalizes the lack of ethics of corporate criminal conduct is that on numerous occasions companies such as IBM,

Facebook, and Google[3] trained their tools, which made use of AI, under false pretenses, as verified with *DeepFace*, which was banned in Europe (Bridle, 2019, p. 161).

It is alleged that we are facing an existential crisis of humanity in its dialogue with AI, since some simple questions are not being answered. So what happens when important decisions are transferred to a system built by a few people, when such decisions affect the whole of society? However, a second question would be: what happens when these decisions are influenced by biases of market forces or political interests? Or should these unethical practices such as the regularity of the technological treatment of human beings be normalized? These questions show the scant reflection on the directions of the technological development of AI, both in its propositions and in its consequences (Webb, 2019, p. 15).

Although the aforementioned questions are aimed at AI, they are easily applied to other technological tools, such as algorithms, machine learning, among other fields of practical inflection in the governmentality of life. Likewise, the absence of a deepening of the aforementioned issues reveals the risks of technological displacement to the punitive field and to state surveillance. There is, therefore, an irresponsibility in the implementation of mechanisms produced mainly by an unethical paradigm (without taking up rights violations), and when applied to models of control they reinforce articulations of death, discrimination, violence and oppression, formatting an ethical co-responsibility for the social damage between creators of new technologies, companies, public managers and agents of the penal system.

The State-business links already evidenced in the police field, as Brayne (2021, p. 39) clarifies, were also presented in the studies by Raji (*et al*., 2020) with an emphasis on facial recognition software. Although facial processing technology (FPT) is praised, listing the benefits of its application, reality reveals the vulnerability of these systems to abusive, racist and discriminatory actions, especially in the field of surveillance/security, also relying on the collection of predatory data from the target population. This is significant when companies like Amazon and HireVue negotiate with states to provide instruments like this to criminal enforcement agencies.

In addition, in the evaluation of facial processing technological tools, the ethical issues of lack of consent in the use of facial images used by the IBM instrument (Diversity Faces) were also denounced. In this case, a licensed image bank, Flickr, was used, but although the images are publicly accessible online, this does not mean consent for their insertion "in a facial

[3] Google has a history of violating practices, as reported in 2018 in the case of storing user locations, even when they had disabled the location history option (Véliz, 2020, p. 29).

recognition database". Another point found was that violations of privacy and consent for databases are usually disproportionately found against people from marginalized groups (Raji, *et al*., 2020, p. 148).

It is healthy to note that the unethical and cooperative nature between companies and states in unauthorized tests, and intended for the service of criminal control, was also verified in Brazil, as happened in cities such as Rio de Janeiro, São Paulo and Salvador. It is mentioned that the actions were duly advised by companies, such as OI (and indirectly Huawei), which even with ineffective results (96% of the alerts in the Salvador carnival did not result in any effective action by public security), ended up praising the "success" of the device (making an arrest based on facial recognition) (Elesbão; Saints; Medina, 2020, p. 252 – 253). The apparent success obscures ethical questions in the research, and more precisely whether this type of technology could be used without the authorization of those involved, reducing everyone to "free" guinea pigs. Would it be feasible to consider it ethical conduct to experiment with the public with something that malfunctions, with discriminatory biases and with numerous defects? These types of questions are based on one of the most basic elements of empirical research with human beings, that is, what are the risks and benefits that justify the study.

4 Technoethics and deliberate blindness of criminal-technological control

The reflections on the legal and ethical violations mentioned above reinforce the conception that the insertion of this type of components in an equation historically composed of an illegitimate (Zaffaroni, 2001, p. 16-17) and violent penal system model, offers an inconsequential and harmful continuity for the population, and such violations are hidden by technological myths, lack of respect for ethical norms of research with human beings and intentional ignorance about the field of technoethics.

This last aspect deserves attention, since the ethical concern in relation to technology cannot be considered a recent reflection, given the debates that date back to the 1970s (and that have ramifications – nanoethics, infoethics and bioethics) and that already focused on the issue of the attribution of responsibility for the creation and effects of technologies by their creators (Echeverría, 2010, p. 144). Therefore, from the appreciation of authors who seek to define the term technoethics, it is possible to verify their approach to a conception linked to interdisciplinarity and that aims to consider the ethical-moral aspects of technology inserted in

the most varied social spaces, while reflecting on the purposes of these instruments. This means that those who debate technoethics do not face a consequentialist model, that is, they are simply attentive to the risks/dangers generated by technological innovations, but reflect on research, how it is used, creation and the possible benefits for human beings and the planet (Vivas, 2018, p. 240).

The current state-business stance on technology is constituted by the violation of research resolutions or legal regulations, as well as by the intentional ignorance of an entire area that would modify the technological projection in society, something similar to what happens in issues related to the debate on global warming and the contestation of climatology (Dias, 2021a).

In this sense, Krutka, Heath and Willet comment that when taking technoethics, the social implications of technologies are projected, so this perspective must be in the foreground and accompany the development of any innovation. However, the conduct of technology markets seems to be more aligned with the scientific situation exposed in the work of fiction *Jurassic Park*, that is, the focus is on the possibility of doing something and not on whether it should be done and, therefore, thinking about avoiding the damage derived from this same possibility (Krutka; Heath; Willet, 2019, 556).

Next, the authors raise the importance of this technoethical reflection when thinking about the insertion of technologies in the field of education, since if such a consideration does not surround those who idealize such devices, an unethical pattern could not be followed in the field of applications of these instruments with people in the development phase (Krutka; Heath; Willet, 2019, p. 557). Thus, although there is a direction in this observation, it could be extended to numerous fields of the legal-criminological plane, which would necessarily include adoptions by the penal system, through public security.

However, it is pertinent to say that this perspective seeks to overcome mere obedience to rules as an ethical path in technology, something that already happens with ethical verification systems (example of *The Ethical OS-SO),* but which end up resulting in the same considerations, reflections and subjects (technical ideal) manifesting themselves on the subject (Amrute, 2019, p. 58). For this reason, the technoethical position, now defended, dialogues with propositions that call for technodiversity, as Hui teaches when he states that "we will need to return to different modes of knowledge that have not yet been considered by engineers and academics" (Hui, 2020, p. 186).

Similarly, there is Amrute's proposal, which brings the need to think of technoethics as a field capable of including the contributions of beings affected by the digital economy. This means that the idea of her conception of techno-affects starts from the feminist matrix to compose constant critical resignifications of the technological field and the reflection of what would be a necessary technoethics for the formation of new forms of life in society, something that to a certain extent inverts the dynamics of criticism, starting from the aggrieved, those affected by penal control or the victims of social damage, to oppose the technological regimes of capitalist exploitation (Amrute, 2019, p. 57).

From these approaches, it is perceived that there is no concern on the part of private or public agents that implement technological devices at the social level, including the field of punitive surveillance, no concern for technoethics, so that those who suffer the consequences of these instruments are once again ignored. For logical reasons, when this is extended to the mechanisms of social control, the invisibilities of the same people and social groups already denounced in the criminological field are repeated, so that those affected cannot influence, speak or oppose the "innovations" of the surveillance model.

Therefore, the lack of ethics in corporate-technological action in research with human beings and the intentional ignorance of technoethics work in favor of the reinforcement of the general articulations of capitalist control and surveillance; At the same time, when these technological tools are transferred to the penal system, the dynamics of violence, discrimination and death are reiterated, duly endorsed by state permission, as well as its agents who defend these receptions, aware of the social damage derived from them and their production through the lack of technological ethics.

5 Conclusion

The realization of a critical assessment always imposes the challenge of rethinking, and this is something that becomes verifiable in the approach to criminal control in a data capitalism based on surveillance and the resulting effects of corporate-technological practices on the population. It is necessary to abandon the dogmas and myths that surround the technological universe, in order to carry out an updated reading of the ways of governing subjects and populations, while at the same time verifying the continuous connection between economic ends and social control, enhanced by technopolitics.

That said, returning to the initial question about the existence of a standardization of the lack of ethical respect and the invisibility of social damage in the corporate production of technologies, especially those linked to the penal system, the question can be answered affirmatively.

Although the allusion to the problems and deviations found in the system of surveillance capitalism allowed the conclusion to be tilted, they had the contextual role of presenting the behavior of the current economic model, demonstrating that despite the permanence of profitability and other basic features, we are facing another composition. The adaptable nature of capitalism is reiterated in the operability of data-based surveillance and in the discursive softening that naturalizes the abusive control of human life in society, communicating phenomena as something inevitable, without alternatives.

However, when we focus on two ethical pillars of observation, unethical practices become undeniable. This leads to the conclusion of the truthfulness that one has in one's hands a *Modus operandi* of the technology industry, making use of protections, immunizations, among other facilities, to not respect the ethical bases in research with human beings, provided for in national regulations, as well as not to appreciate technoethics as a scientific field of critical contestation of such innovations.

Finally, the passage of this unethical archetype affects the instruments applied to criminal control, adding one more layer to the repeated problems that delegitimize a system that is known to be illegitimate and produces social damage. It means that today surveillance databases produce various damages to the population (health, education, work, privacy, etc.), but that when they are put at the service of the punitive field they reinforce discrimination and violence fueled by unethical components and turning the defenders of these irresponsible "innovations" into co-authors of the violations/damages produced.

References

AMARAL, Augusto Jobim do; MARTINS, Fernanda; ELESBÃO, Ana Clara. Algorithmic racism: an analysis of whiteness in digital image banks. **Pensar-Revista de Ciências** Jurídicas, Fortaleza, v. 26, n. 4, p. 1-9, out./dez. 2021. Available in: https://ojs.unifor.br/rpen/article/view/11806/6702. Access date: 15 Jan. 2022.

AMARAL, Augusto Jobim. **Criminology policy**. São Paulo: Tirant Lo Blanch, 2020.

AMOORE, Luisa. **Cloud ethics** : the algorithms and attributes of ourselves. London: Duke University Press, 2020.

AMRUTE, Sareeta. Of techno-ethics and techno-affects. **Feminist Journal**, Thousand Oaks, v. 123, n. 1, p. 56-73, 2019. Available at: https://journals.sagepub.com/doi/pdf/10.1177/0141778919879744. Access date: 16 Nov. 2021.

BARAK, Greg. The crimes of the powerful and the globalization of crime. **Revista Brasileira de Direito,** Passo Fundo, v. 11, n. 2, p. 104 – 114, jul./dez. 2015. Available at: https://seer.atitus.edu.br/index.php/revistadedireito/article/view/931/721. Access date: 21 Jan. 2022.

BEIGUELMAN, Giselle. **Politics of the image**: surveillance and resistance in the datasphere. São Paulo: Ubu, 2021.

BERARDI, Franco "Bifo". **Asphyxiation**: Financial Capitalism and the Insurrection of Language. São Paulo: Ubu, 2020.

BRAZIL. Ministry of Health. National Committee on Research Ethics. **National Health Council**, Brasilia, 2021. Available in: http://conselho.saude.gov.br/comissoes-cns/conep/. Access date: 21 Nov. 2021.

BRAZIL. Ministry of Health. **Resolution 466, of December 12, 2012**. Brasilia, DF: National Health Council, 2013. Available at: https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf. Access date: 21 Nov. 2021.

BRAZIL. Ministry of Health. **Resolution 510, of April 7, 2016**. Brasilia, DF: National Health Council, 2016. Available in: http://conselho.saude.gov.br/resolucoes/2016/Reso510.pdf. Access date: 21 Nov. 2021.

BRAYNE, Sarah. **Predicting and Monitoring**: Data, Discretion, and the Future of the Police. New York: Oxford University Press, 2021.

BRIDLE, James. **The new dark age**: technology and the end of the future. São Paulo: Still, 2019.

BROWN, Wendy. **In the Ruins of Neoliberalism**: The Rise of Anti-Democratic Politics in the West. São Paulo: Filosófica Politeia, 2019.

BUDÓ, Marília de Nardin. Silenced Harm: The Banality of Evil in the Scientific Discourse on Asbestos. **Revista Brasileira de Direito**, Passo Fundo, v. 12, n. 1, p. 127-140, Jan./Jun. 2016. Available at: https://seer.atitus.edu.br/index.php/revistadedireito/article/view/1281/843. Access date: Dec 19 2021.

CHIGNOLA, Sandro. Life, Work, Language: Biopolitics and Biocapitalism. **Cadernos IHU,** São Leopoldo – RS, year 13, v. 13, n. 228, p. 3-19, 2015. Available at: http://www.ihu.unisinos.br/images/stories/cadernos/ideias/228cadernosihuideias.pdf. Access date: 01 Jan. 2022.

CHIGNOLA, Sandro. **Foucault beyond Foucault**: a politics of philosophy. Porto Alegre: Human Creation, 2020.

CRARY, Jonathan. **24/7**: Late capitalism and the end of the dream. São Paulo: Ubu, 2016.

DELEUZE, Gilles. "Post-scriptum" on the holding companies. *In*: DEULEUZE, Gilles. **Talks:** 1972-1990. 3rd ed. São Paulo: Editora 34, 2013. pp. 223-230.

DIAS, Felipe da Veiga. Technopolitics and the death of sustainability: mythomania as a response to the limits of the planet. **Argumentum Revista de Derecho**, Marília, v. 22, n. 2, p. 487-505, 2021a. Available at: http://ojs.unimar.br/index.php/revistaargumentum/article/view/1295/895. Access date: 20 Nov. 2022.

DIAS, Felipe da Veiga. Prediction algorithms in the penal system: the technopolitical prophecies that self-fulfill in the twenty-first century. **Brazilian Journal of Criminal Sciences,** São Paulo, v. 29, n. 183, p. 99-124, September 2021b.

DIJCK, José Van. **The culture of connectivity**: a critical history of social networks. Buenos Aires: Siglo Veintiuno editores, 2016.

ECHEVERRÍA, Javier. Technoscience, technoethics and technoaxiology. **Revista Colombiana de Bioética**, Bogotá, v. 5, n. 1, p. 142-152, 2010. Available at: https://www.redalyc.org/pdf/1892/189217244009.pdf. Access date: 20 Nov. 2022.

ELESBÃO, Ana Clara Santos; SANTOS, Jádia Larissa Timm two; MEDINA, Roberta da Silva. When the (facial recognition) masks fall, it will be a big carnival. *In*: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldiserra Carvalho (coord.). **Algorithmisms**. São Paulo: Tirant lo Blach, 2020. pp. 261-273.

FISCHER, Marcos. **Capitalist realism**: is it easier to imagine the end of the world than the end of capitalism? São Paulo: Autonomia Literária, 2020.

FOER, Franklin. **The world that does not think**: humanity in the face of the real danger of the extinction of homo sapiens. Rio de Janeiro: Leya, 2018.

FOUCAULT, Michel. **What is criticism? [Review and Aufklärung]**. [*S. l.: s. n.*], 1978. Available at: http://michel-foucault.weebly.com/uploads/1/3/2/1/13213792/critica.pdf. Access date: 16 Jan. 2022.

FOUCAULT, Michel. **Security, Territory, Population:** Course at the Collège de France (1977-1978). São Paulo: Martins Fontes, 2008.

HARCOURT, Bernard E. **Exposed**: Desire and Disobedience in the Digital Age. Cambridge: Harvard University Press, 2015.

HUI, Yuk. **Technodiversity**. São Paulo: Ubu, 2020.

KUCHARSKI, Adán. **The rules of contagion**: why things spread and why they stop spreading. Rio de Janeiro: Record, 2020.

KRUTKA, Daniel G.; HEATH, Marie K.; WILLET, K. Bret Staudt. Close-up of technoethics: Towards critical perspectives in technology and teacher training. **Journal of Technology and Teacher Education,** Waynesville, v. 27, n. 4, p. 555-574, 2019. Available at: https://www.learntechlib.org/p/208235/. Access date: 20 Nov. 2021.

LAMA, José Pérez de; SANCHEZ-LAULHE, José. Considerations in favor of a broader use of the term technopolitics On the need for critique and politics of knowledge and technologies. *In*: SABARIEGO, Jesús; AMARAL, Augusto Jobim do; SALLES, Eduardo Baldiserra Carvalho (coord.). **Algorithmisms**. São Paulo: Tirant lo Blach, 2020. pp. 19-43.

LARRAURI, Elena. **The Legacy of Critical Criminology**. 2nd ed. Madrid: Siglo XXI Editores España, 1992.

LAZZARATO, Maurizio. **The Factory of the Indebted Man**: An Essay on the Neoliberal Condition. Buenos Aires: Amorrortu, 2013.

LAZZARATO, Maurizio. **Signs and Machines**: Capitalism and the Production of Subjectivity. Los Angeles: Semiotext(e), 2014.

LOVELUCK, Benjamín. **Networks, freedoms and control**: a political genealogy of the internet. Petrópolis: Vozes, 2018.

MOROZOV, Evgeny. **Big tech**: the rise of data and the death of politics. São Paulo: Ubu, 2018.

MOROZOV, Evgeny. **To save it all, click here**: the madness of technological solutionism. New York: Public Affairs, 2013.

NOBLE, Safiya Umoja. **Algorithms of oppression**: how search engines reinforce racism. New York: New York University Press, 2018.

O'NEIL, Cathy. **Weapons of Mathematical Destruction**: How Big Data Increases Inequality and Threatens Democracy. New York: Crown Publishers, 2016.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

RAJI, Inioluwa Deborah; GEBRU, Timnit; T., MITCHELL, Margaret; BUOLAMWINI, Alegría; LEE, Joonseok; DENTON, Emily. Save face: Investigate the ethical concerns of facial recognition auditing. *In*: AIES '20 AAAI/ACM CONFERENCE ON AI, ETHICS, AND SOCIETY, 20., 2020, New York. **Minutes of the** [...]. New York: Computer Machinery Association, 2020. pp. 145-151. Available at: https://dl.acm.org/doi/pdf/10.1145/3375627.3375820. Access date: 01 Jan. 2022.

RUIZ, Castor Bartolomé. Algorithmization of life: the new governmentalization of behaviors. **IHU Ideias Magazine**, São Leopoldo, year 19, v. 19, n. 314, 2021. Available at: https://www.ihu.unisinos.br/images/stories/cadernos/ideias/314cadernosihuideias.pdf. Access date: 20 Dec. 2021.

SARMIENTO, Camilo Ernesto Bernal; CABEZAS, Sebastián; FORERO, Alejandro; RIVERA, Iñaki; VIDAL, Iván. Beyond Criminology: An Epistemological Debate on Social Harm, International Crimes, and Market Crimes. *In*: RIVERA, Iñaki (coord.). **State crimes, markets and social damage**: debates in critical criminology and legal-criminal sociology. Barcelona: Anthropos, 2014. pp. 35-80.

SCHNEIER, Bruce. **Data and Goliath**: the hidden battles to collect your data and control your world. New York: W.W. Norton & Company, 2015.

SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity Press, 2017.

SUMPTER, David. **Dominated by numbers**. Rio de Janeiro: Bertrand Brasil, 2019.

TAYLOR, Ian; WALTON, Pablo; YOUNG, Jock. **The New Criminology**: Contribution to a Social Theory of Deviant Behavior. 3rd ed. Buenos Aires: Amorrortu, 2007.

VÉLIZ, Carissa. **Privacy is power**. Great Britain: Penguin Random House, 2020.

VIVAS, Willy Jharinton. Safe and responsible use of ICTs: a technology-based approach. **Ciencia, docencia y tecnología**, Concepción del Uruguay, v. 29, n. 57, p. 235-255, Nov./Apr. 2018. Available in: http://www.scielo.org.ar/pdf/cdyt/n57/n57a10.pdf. Access date: 15 Nov. 2021.

WEBB, Amy. **The Big Nine**: How the Titans of Technology and Their Thinking Machines Could Warp Humanity. New York: PublicAffairs, 2019.

ZAFFARONI, Eugenio Raúl. **In Search of Lost Sentences**: The Loss of Legitimacy of the Penal System. Rio de Janeiro: Revan, 2001.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Struggle for a Human Future on the New Frontier of Power. New York: PublicAffair, 2019.