# *Technolatry and Virtual Emotions* in the Era of *Digital Brutalism*: Understanding the proliferation of Cybercrimes in *Modern* Brazil

**Siddharth S.M.Bora**
Faculty of Economics, University of Coimbra

Artigo recebido a 08/02/2025.
Aceite para publicação a 04/06/2025.

## Abstract

In modern Brazil, technology has shifted from a tool of progress to an object of near-religious reverence what Achille Mbembe calls *Technolatry*. This uncritical veneration fosters dependence and shapes virtual emotions tied to digital life. Brazil's rise in cybercrimes reflects a legacy of colonial algorithmic exploitation, data surveillance, and the weaponization of online anonymity. This study explores the symbiotic relationship between technology and crime, revealing how Brazil's socio-political landscape is being redefined. By examining this digital transformation through a sociological lens, I aim to highlight the broader political and societal impacts, offering a case study that encapsulates this complex dynamic

**Palavras-chave:** Technolatry; Virtual Emotions; Cybercrimes in Brazil.

## *Tecnolatria e Emoções Virtuais na Era do Brutalismo Digital: Compreendendo a Proliferação da Cibercriminalidade no Brasil Contemporâneo*

## Resumo

No Brasil moderno, a tecnologia deixou de ser apenas uma ferramenta de progresso para se tornar um objeto de veneração quase religiosa que Achille Mbembe denomina de Tecnolatria. Essa adoração acrítica gera dependência e molda emoções virtuais ligadas à vida digital. A ascensão da cibercriminalidade no Brasil reflete um legado de exploração algorítmica colonial, vigilância de dados e uso estratégico do anonimato *online*. Este estudo explora a relação simbiótica entre tecnologia e criminalidade, revelando como o cenário sociopolítico brasileiro está sendo redefinido. Por meio de uma abordagem sociológica, a pesquisa destaca os impactos políticos e sociais mais amplos, ilustrados por um estudo de caso.

**Palavras-chave:** Tecnolatria; Emoção digital; Cibercriminalidade no Brasil.

BORA, Siddharth S.M. (2025),
"Technolatry and Virtual Emotions in the Era of Digital Brutalism: Understanding the proliferation of Cybercrimes in Modern Brazil",
*Sociologia: Revista da Faculdade de Letras da Universidade do Porto,* Vol. LI, pp. 95 - 124
DOI: https://doi.org/10.21747/08723419/soc51a4

## *Technolâtrie et Émotions Virtuelles à l'Ère du Brutalisme Numérique: Comprendre la Prolifération de la Cybercriminalité dans le Brésil Contemporain*

**Résumé**

Dans le Brésil moderne, la technologie est passée d'un outil de progrès à un objet de vénération quasi religieuse ce qu'Achille Mbembe appelle la *Technolâtrie*. Cette adoration non critique engendre une dépendance et façonne des émotions virtuelles liées à el vie numérique. La montée de la cybercriminalité au Brésil reflète un héritage d'exploitation algorithmique coloniale, de surveillance des données et d'armement de l'anonymat en ligne. Cette étude explore la relation symbiotique entre technologie et criminalité, révélant comment le paysage sociopolitique brésilien est redéfini. À travers une approche sociologique, l'étude met en lumière les impacts politiques et sociaux plus larges, illustrés par une étude de cas.

**Mots-clés:** Technolâtrie ; Émotion numérique; Cybercriminalité au Brésil.

## *Tecnolatría y Emociones Virtuales en la Era del Brutalismo Digital: Comprendiendo la Proliferación de los Ciberdelitos en el Brasil Contemporáneo*

**Resumen**

En el Brasil contemporáneo, la tecnología ha dejado de ser solo una herramienta de progreso para convertirse en un objeto de veneración casi religiosa, fenómeno que Achille Mbembe denomina *Tecnolatría*. Esta devoción acrítica genera dependencia y moldea emociones virtuales vinculadas a la vida digital. El aumento de los ciberdelitos en Brasil refleja una herencia de explotación algorítmica colonial, vigilancia de datos y uso estratégico del anonimato en línea. Este estudio investiga la relación simbiótica entre tecnología y crimen, revelando cómo se redefine el panorama sociopolítico brasileño. A través de una mirada sociológica, se examinan los impactos políticos y sociales más amplios, ilustrados mediante un estudio de caso.

**Palabras clave:** Tecnolatría; Emoción Digital; Ciberdelitos en Brasil.

*In the pulse of circuits, humanity merges.*
*The self, once solid, now a blur*
*We walk between two worlds at once,*
*Data flows, a steady stream,*
*Our hearts are coded,*
*Our identity built on a screen.*
*Behind the veil, we hide and pretend,*
*But who we are? and who spies us?*
*Are we the authors of our choice?*
*In each algorithm, a silent voice,*
*The warmth of touch, the depths within,*
*Replaced by screens, a past we can't erase*
*HumanMachina, we are now both whole,*
*Where once was soul, now there is no more.*

## Introduction

*Digital Brutalism* emerges as an analytical framework for examining the oppressive manner in which digital systems are used in *south economies*. This concept draws from Achille Mbembe's (2021) use of the term *Brutalism*[1]. By reframing this notion *Digital Brutalism* reveals the dehumanizing logic embedded in the contemporary digitalized world. *Technolatry* is the near-religious reverence of technology, perceived as *infallible* and as a solution to all social, economic and political issues. In a sense, society's devotion puts technology in a sacred status,

[1] According to Goldhagen & Legault (2000), *Brutalism* is an architectural style that emerged in Europe after World War II, between the 1950s and 1960s. The term comes from the French *béton brut*, which means "raw concrete". Achille Mbembe does not directly reference *Brutalism* in the architectural sense; instead, his work often uses terms like *brutality* metaphorically to discuss structures of power, violence, and oppression. Mbembe's framework aligns with the systemic violence and oppressive practices that create environments of control and dehumanization.

BORA, Siddharth S.M. (2025),
"Technolatry and Virtual Emotions in the Era of Digital Brutalism: Understanding the proliferation of Cybercrimes in Modern Brazil",
*Sociologia: Revista da Faculdade de Letras da Universidade do Porto,* Vol. LI, pp. 95 - 124
DOI: https://doi.org/10.21747/08723419/soc51a4

often disregarding its partiality and limitations to certain situations. This technological determinism frames digital innovation as the driving force of progress and human evolution.

*Virtual emotions* are the product of this paradigm, which are shaped and reshaped, according to the rhythm, speed, and logic of the social/technological engagements it creates. In the digital realm, not all human emotions find a place. Some are considered "unnecessary" and thus do not manifest as *Virtual Emotions*. *Apathy, fear, love,* and *hate* dominate these digital spaces. These emotions, stripped of their complexities, circulate freely, shaping our interactions in a world that often prioritizes speed and efficiency over depth.

*Modern Brazil* is a nation-state shaped by its historical legacies of colonialism, slavery, and socio-political stratification that intersect with contemporary processes of globalization, urbanization, and technological innovation. In the context of this study, *Modern Brazil* is particularly viewed through the lens of its *semi-peripheral status*[2] in which it is marked by its dependency on technological imports and external innovations while dealing with internal socio-economic asymmetries. Cyber elements, like *ransomware*, *phishing*, *deepfakes*, and *fake news*, each exemplify crimes that exploit the vulnerabilities that can be used against this fragile system in south economies, where technological consciousness and cybersecurity infrastructures are often underdeveloped.

I adopt a qualitative and exploratory methodology, rooted in theoretical-conceptual analysis and enriched by selected case studies of cybercrime. The cases are not random but were curated to reflect the digital contradictions and technological vulnerabilities that typify semi-peripheral contexts like Brazil. Selection followed three primary criteria: (a) significant national or international impact; (b) direct connection to mechanisms of digital surveillance and/or violations of digital rights; (c) availability of secure, verifiable sources such as technical reports, reputable news outlets, and public documents. In this way, the study maintains a

[2] According to Wallerstein (2004), *semi-peripheral economies* refer to countries or regions that are positioned between the developed (core) and underdeveloped (peripheral) nations within the global economic system.

predominantly theoretical orientation, while remaining critically attuned to the real-world effects of digital systems in postcolonial and semi-peripheral societies.

In the first section, the paper will provide a theoretical framework for our concepts of *Technolatry* and its direct counterpart *Digital emotions,* analyzing how they have positioned themselves as ideological forces that govern modern social interactions and cultural production in today's digital world. In the second section, the paper will then delve into Brazil's social context, examining how digital technologies have become embedded in the operations of cybercriminality. In the last section, I will present a few case studies on cybercrime Brazil, illustrating how digital tools are used to facilitate illegal activities, *untraceability*, and impunity.

## 1. Brutalism and the Artificial Becoming

In the *Digital Age,* the neoliberal rationality is a compulsory machine of expansion driven by profit and the gradual devaluation of human/nature. Mignolo (2017) argues that Modernity is intrinsically linked to *Coloniality*, stating that decolonial thought emerges as a theoretical counterpoint, offering a perspective of belonging to those who have been and continue to be subordinated *(subalternos)*[3] [4]. When viewed through this lens, Brutalism emerges as a political and philosophical concept that transcends its architectural origins. Mbembe (2021) theorizes that this radical political project seeks to transform the material world, and the human bodies that inhabit it, from *body to soul*, as they see fit. It is a paradigm created through the entrenchment of the neoliberal agenda that promoted its predictive cyclical force to *destroy* and *recreate* society in its own vile manner.

[3] For Spivak (99) *colonialism (imperialism)* has shaped dominant forms of *knowledge* and *power*. In some areas, particularly when examining the manipulation of *law* and *history*: "Writing in the metropolis or in the former colony, many of us are trying to carve out positive negotiations with the *episteinic* graphing of imperialism. For some of the shadow areas in the *Inicrology* of the manipulation of law and history, cutting across the body of the great narrative of imperialism, no good word can be said (p.80)"

[4] Mignolo's body of work reflects how, on the different stages of humanity each level of *interconnectedness*, culminated in the contemporary scenario of our current world, deeply interconnected by *globalization*, *modernity*, and *coloniality* (Mignolo, 2017).

*Brutalism*'s political dimension intersects with global movements of *demolition* and *renewal*, particularly in marginalized areas where the intersection with technology produces new forms of exploitation (Mbembe, 2019). According to Mbembe (2021):

> "*Brutalism* is the name given to this gigantic process of dumping and evacuation, but also of unloading the containers and emptying the organic substances. Destructive creation." (p. 15)

The dialectic between *destruction* and *reconstruction* is central in *Brutalism* and it's deeply connected to broader processes of global demolition and ecological degradation. Mbembe (2021) understands that "environmental devastation is not a coincidence but the direct result of centuries of colonial and industrial exploitation that prioritized profit over life" (2021, p. 67). *Brutalism* reflects the broader global transformations that are reshaped by both the *biosphere* and *Technosphere*[5]. Mbembe (2021) states,

> "These transformations of the biosphere and the *Technosphere*. This process, which has triggered unprecedented tremors, is global. Its goal is to precipitate the mutation of the human species and accelerate its transition to a new condition, both plastic and synthetic, and consequently, malleable and extensible. To organize the passage to a new terrestrial dispensation (a new nomos of the Earth), eventually replacing it with a nanoworld, that of cellular, neuronal, and computational devices. A world of plastic tissues and synthetic blood, it will be populated by bodies and entities that are half natural and half artificial." (p.15)

These transformations on *human bodies*[6] and in their *lives* are reconfigured by economic, technological and political systems. According to Mbembe (2021), "we live in a time when the body is increasingly modified, monitored, and exploited by technology, from data extraction

[5] Mbembe often engages with the idea of *Technosphere* in the context of his broader theories of *Necropolitics*, where technology and systems of power (e.g.,surveillance, military technology, bioengineering, and digital networks) are used to control, discipline, and even determine who is allowed to live and who is subjected to forms of social and political death. The T*echnosphere*, for Mbembe, is not just a set of technological innovations but a mechanism through which power is exerted, and through which modern forms of violence and exclusion are organized.

[6] According to Mbembe, "the logics of fracturing and fissuring, one must also add those of exhaustion and depletion. Once again, fracturing, fissuring, and depletion refer not only to resources but also to living bodies exposed to physical exhaustion and to a wide range of biological risks, often invisible, acute intoxications, cancers, congenital anomalies, neurological disorders, hormonal disruptions." (p. 15)

to genetic manipulation" (p.105). The accelerating pace of technological advancement and the degradation of the environment are interconnected with the rise of global capitalism and colonial histories that exacerbate social inequalities and *environmental destruction*. The impact of these brutal transformations is evident in the socio-political dynamics of contemporary globalization, where the boundaries between the human and the non-human, the natural and the artificial are increasingly blurred. As the planet faces unprecedented environmental challenges, the brutality of global capitalism is laid bare, with entire ecosystems and populations being sacrificed in the name of *progress*.

### a) The Digital Rationality and the Demythologization of the World

The rise of digital technologies represents a shift from mythological understandings of the world to a more technocratic worldview, one in which knowledge and truth are increasingly governed by data, algorithms, and the rationality of computational systems (Mbembe, 2021). This *digital rationality* fosters a world where the complexity of human experience is reduced to quantifiable elements, stripping away the *cultural* and *symbolic* frameworks that once provided *meaning*. Mbembe (2021) argues that the world has become increasingly mediated by digital systems and that the ability to *mythologize* or *create* alternative narratives has faded, *disintegrated*, leaving individuals exposed to a reductionist, rationalized conception of the *world*.

*Demythologization*[7], a conceptual landmark, shows us how contemporary power structures are maintained and reinforced, especially in semi-peripheral economies, like Brazil. Mbembe suggests that in the digital realm, being human is redefined. The process of *demythologization*, therefore, involves not only the erosion of spiritual or narrative forms of knowledge but also the imposition of a form of digital governance that seeks to regulate,

[7] In Mbembe's perspective, *demythologization* refers to the process of stripping traditional societies and cultural systems of their mythical, spiritual, and symbolic dimensions, often as a consequence of modernity, colonialism, and technological progress. This concept is particularly tied to the larger critiques Mbembe offers regarding the impacts of capitalism, globalization, and technoscience on post-colonial societies. It is not simply a historical process; it is a contemporary phenomenon deeply tied to the ongoing dynamics of power, technology, and globalization. It shapes how societies conceptualize life, death, and community in the *modern era*.

control, and manipulate reality itself. Hence, by dismantling traditional myths and cultural narratives, *Digital rationality* facilitates a vision of the world that is not a lived experience of individuals but an increasingly regulated technological society that serves the interests of *global capital*[8] and *state power* (Mbembe, 2019). This transformation is central to the experience of those living in Brazil, where this "evolution" leads to the assertion of structural inequalities and the reinforcement of old forms of colonial social hierarchy now rooted in *algorithmic control*.

### b) *Technolatry* as Ontological Destiny

The reverence of technology becomes an existential condition, shaping both the *physical* and *symbolic dimensions* of the human experience. The omnipresence of technology in daily life and its integration into both the human body and its environments suggests that a future where human life is inextricably dominated by technological systems is inevitable. *Technolatry* is thus an *ontology of domination*, not as a mere instrument but as a central force that shapes the future of all existing life on earth. This ontological shift is a reflection of a deeper crisis in modern human existence against a *spiritless* opponent and one that can destroy and reconstruct at the velocity of global capitals request.

*Technolatry*[9] is an *all-conscious* societal state of mind that places technology as an encompassing *force*. It is the lens through which the world is now viewed, and, ultimately, the one through which the world will be *governed*. This reconfiguration reflects the ascendancy of machine *logic* over human *intuition*, reducing individuals to mere components in a larger system of technological governance. This transformation is not merely about the

[8] Adding to this perspective, Zuboff (2019) adds that this new economic global order processes human experience as a *free raw material* for the *capitalist machine*. A parasitic economic logic in which the production of goods and services are subordinated to a global architecture of behavioral modification and parametrization. A movement that aims to impose a new collective order based on *total certainty*. An expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty.

[9] According to Mbembe (2021) technology is today a reality that is simultaneously material and immaterial, psychic, personal, and internal. It no longer belongs to the external world, a membrane defining the boundary between the interior (humanity) and the exterior (nature). It is our clinic, the place where, in its somber clarity, three constitutive realities of the living world manifest themselves: the biological, organic, vegetal, and mineral reality of bodies of any species; the psychic reality of affections; and the social reality of exchanges, language, and interactions. (p.43)

material world; it entails a profound redefinition of what it means to be human and machine [10]*, HumanMachina*[11]*.* These processes are about the redefinition of *human subjectivity* in relation to its natural world. Therefore, *Technolatry* is more than just an attachment[12] to technology; it is a relentless *modus operandi of technology's rationality*[13].

### c) *Virtual Emotions* and *Digital Surfaces*

Ahmed (2004) suggests that *emotions* are shaped by collective practices and, in this way, play a significant role in the construction of identities and power dynamics within any given society. Hence, the relational nature of *emotions* is determined by *emotional orientations*, which influence our *physical surface* (bodies), in turn influencing ourselves both physically and socially.

> "Emotions shape the surfaces of bodies, which take form through the repetition of actions over time, as well as through orientations toward or away from others. Indeed, paying attention to emotions can show us how all actions are reactions, in the sense that what we do is shaped by the contact we have with others" (p. 35).

[10] According to Boyer (2019) this reduction of the human condition to mechanical and calculable elements aligns with the devaluation of human subjectivity and agency, as the individual becomes a mere cog in a larger technological machine that determines the trajectory of their life, their body, and their very essence.

[11] I see *HumanMachina* as a paradigm of the *self* where individuals are increasingly influenced, shaped, and controlled by technological forces that are both internal and external. As technology advances, the human *body* and *mind* becomes more intertwined with the *digital machine*, leading to a deconstruction of old outdated notions of the *self*. The infinite possibilities guide our emotional experiences to a symbiotic relationship with technology in which algorithms mimics "human essence"and creates *digital avatars* to reproduce *human existence*. This fusion is most evident in the growing ambition of billionaires to transcend biological limitations through technology. *Bioengineering, neural interfaces*, and *artificial intelligence* are forms to merge consciousness with the *digital machine* in a pursuit of *digital immortality*. The body is no longer a singular biological entity but a node in a vast cybernetic network where identity is *fractured*, emotions quantified, and instrumentalized. As this fusion accelerates, a question arises: is humanity evolving, or is it being rewritten?

[12]Mbembe (2021) understands that it is through technology that the activities of thought and the work of figuration, symbolization, and memorization take place. (p.43). There is almost no longer any division between the human and the technical object, the thing. From now on, the human is no longer merely coupled with the machine, matter, and the object. They are no longer simply nestled in its folds and creases. They have literally found within them the privileged sites of their incarnation, and these, in turn, are in the process of being covered, if not with their face, at least with their mask (p.45).

[13] Mbembe (2019) understands that this shift, while promising new forms of existence, also condenses the fragility and vulnerability of more marginalized humans, who aggressively bear the brunt of these transformations.

The relational nature of emotions is all a part of a broader understanding of how they are formed and expressed in the external world. In this context, *Emotions* are not isolated experiences because they are shaped by the interactions and orientations of individuals toward specific *objects* and *motivations* (Ahmed, 2004):

> "In other words, emotions are neither inside the individual nor the social; rather, they produce the very surfaces and boundaries that allow the individual and the social to be delineated as if they were objects. My analysis will show how emotions create the very surfaces and boundaries that allow all types of objects to be delineated. The objects of emotion take form as effects of circulation" (p. 12).

*Emotions* are produced through everyday encounters in social life, that shape bodies and minds through processes of repetition (Ahmed, 2004). In the digital sphere, this means that society makes emotional connections through technologies, platforms, and interfaces, generating emotional significance through affective technological attachment.

In the digitalized world individuals are increasingly influenced, shaped, and controlled by technological forces. In this sense, artificial intelligence, virtual reality, and data-driven systems are *extensions* of our cognitive and emotional faculties. Human identity may no longer reside in the organic body but in the biotechnological systems that breed it, improve it and sustain it. Technology offers new forms of interaction, but it also diminishes the depth and complexity of traditional human connection. Genuine emotional experience and digitally-mediated simulation become unrecognizable, emotional bonds are redefined and personal connections are *transformed*.

According to Simmel (1950), the *blasé attitude* is that invisible armor which silences astonishment, muffles affect, and turns the world into something devoid of both *brilliance* and *pain*. Bringing this understanding to the digital realm, this indifference evolves like an organism adapted to the vertigo of screens. The soul, confronted with infinite windows, learns not to feel.

Lipovetsky (2005), with his lucid melancholy, captured the modern era as a time in which everything is permitted, yet nothing truly matters. He understands apathy today is not

absence, but *excess* of stimuli, of choices, of possibilities. In the virtual world, it settles like a fog that anesthetizes the *spirit*. We *love without bodies*, *hate without faces*, and *cry with emojis*. This digital apathy is the twin sister of the blasé; it does not reject the world, but consumes it without digesting, touches it without feeling.

Baudrillard (1999) tells us that *the real* is no longer necessary. In place of emotion, we have its holograms and their programmed reactions, *like-driven loves* and *algorithmic knowledge*. We *feel by proxy*, *desire by reflex*. Emotions are no longer experiences, but performances circulating between *avatars*. We live within the *simulacrum*, where tears are animated stickers and affection is a product wrapped in metrics. In this theater of emotional phantoms, the *blasé attitude*, *programmed apathy*, and *digital simulacrum* do not merely coexist, they embrace one another in silence, rocking our humanity to internalize the *Virtual Emotions.*

*Virtual Emotions* are the *ghostly echoes of human feeling*, suspended between the mechanical and the meaningful, the expressive and the empty. They are the anesthetized effect of a digital age, an emotional survival mechanism that both *connects* and *alienates*, *numbs* and *stimulates*, *mirrors* and *masks*. To understand *Virtual Emotions,* one must understand that the term encompasses only a few of the human emotional states. To be specific, a*pathy*, *fear*, *love* and *hate*, which are our most primitive emotions and in *Cyberspace* are, in a way, responsible for the *cyberaffective experience* that it's witnessed.

In this context, *Virtual Apathy*[14] is an engineered state, a byproduct of our digital society. As the constant information overload numbs our minds and leads to *an absence of empathy* for everything and everyone, as well as an emotional indifference to the suffering of others. As society scrolls through its endless content, it testifies to this modern spectacle of pain that gradually dehumanizes[15] our *soul*. But at the same time, I also understand that *Virtual apathy*

[14] Dwelling on Lipovetsky (2005) ´s concept of *Apathy*, I recall that he states "we live in a society of seduction and spectacle, where emotional mobilization is intense but ephemeral, leading more to dispersion than to commitment. The excess of information and stimulation no longer generates awareness but rather anesthesia, saturation, and indifference" (p.45)

[15] According to Baudrillard (1993) we live in a world where there is more and more information, and less and less meaning. (p. 79). Where the image no longer even has the time to become an image, as it is anticipated by

is something that regulates individual social functionality. It's functional, because it allows society to endure this day-to-day digital torture without having something of an emotional burnout. It places our *soul* in a cold, kind of *detached state of mind* that makes it easier to *ignore*, dismiss, and not care. *Virtual apathy* has pronounced our passiveness and our accommodation to everything, *passion* is no more, and today´s *empathy* is slowly forgotten (Lipovetsky, 2005)

*Virtual Fear* is sustained not by immediate danger, but by an endless flood of *uncertainty*, threats that are at the same time invisible, abstract, and *omnipresent*. Data breaches, misinformation, and social media judgments are just some of the elements that help create an environment where one is never sure *who is watching*. *What is real*? *Are we really free? Virtual Fear* is instrumentalized to create more submission, more censoring, and more emotional withdrawal to aid in the ruling of the unseen forces *(*Bauman, 2006; Baudrillard, 1994; Zuboff, 2019).

Society has been remanufactured by *algorithms*, held together by an *illusion*, and fueled by the need for *carnal validation*. *Love* is stripped of depth, reduced to mere gestures of engagement. Online, we see them every day, likes, shares, emojis, and instant audio messages. They are immediate, quantifiable, and transactional gestures that lack the texture of real human relations. *Virtual Love* is the *illusion of connection*. Sexual superficiality mirrors this transformation, and technology turns desire into instant gratification. And *Love*, which once was the reason for the search for emotional ease, now gives way to *Virtual Love* and one-time discardable gratification (Bauman, 1999; 2003). Of course, it is still possible to create meaningful connections with other individuals, but it's just that the probability is much, much lower.

*Virtual Hate*, on the other hand, spreads effortlessly. It thrives on *speed*, *anonymity*, and *virality*. In the digital space, computational algorithms reward polarization, making hate a programmed mechanism of engagement. In the digital world, everyday citizens transform

another image, another flash, which erases the first, and so on. *Speed* is its only essence. (p. 10). A constant exposure to digital content strips us of our emotional impact on any matter.

online platforms into breeding grounds for this dissemination, individuals with *bipolar social conduct* in which one personality conforms to societal norms and the other, embraces the hostility and impunity of the digital realm. What was thought out to be a space for nuanced debate has turned, in digital times, into a free-for-all arena of insults and condemnations *(*Bauman, 2013; Zuboff, 2019).

In the digital realm, *emotions* are not just *felt* but *performed*, *manipulated*, and *weaponized*, reshaping emotional engagement. Each of these emotions is contextualized and reflects the social dynamics of these digital environments. *Virtual Emotions* are a part of the larger fabric of digital culture, influencing the ways in which we navigate and understand the digital realm.

### d) The Brazilian Digital Brutalist experience

*Digital brutalism*, when examined through the lens of semi-peripheral economies, reflects a deeper engagement with the intersection of technological development, social inequality, and global power dynamics. In these economies, the process of adopting new technologies and digital infrastructures is a *brutalist experiment*, where crude, unrefined technological systems are thrust into societies which must adapt quickly to the pressures of global digitalization. These regions often lack the economic or institutional capacity to fully control or regulate technological *flows*, leading to a tension between the technological advances that promise social mobility and the underlying inequalities that such technologies exacerbate (Van Dijlk, 2020).

According to Van Dijlk (2020), these economies may become caught in a *feedback loop* where technological advancement further entrenches their peripheral status within the global capitalist system. It creates a *dual-edged situation*, where, on the one hand, technology holds the potential to bring semi-peripheral economies into closer alignment with global standards of innovation and economic productivity. On the other, the rapid and sometimes brutal incorporation of these technologies into societies ill-equipped to manage them can perpetuate cycles of economic dependency, exploitation, and inequality.

Castells[16] (1996) understands that traditional ways of knowing and organizing society are stripped away in favor of technological solutions that may not align with the realities of semi-peripheral nations. According to Bora (2020), in Brazil the Neoliberal paradigm[17] problems of crime and social inequality are no longer seen as having fundamental causes that can be fixed through policies and resources mobilized by the government, but instead it responds to an economic stimulus brought on by discourse of *cost, profit,* and *disposability.* Another issue is that the introduction of digital technologies often comes without the necessary infrastructure[18], training, or regulatory oversight. This means that these technologies may be applied in ways that prioritize efficiency and productivity over social justice or environmental sustainability.

Brazil's position as a digitally vulnerable country has increasingly made it a testing ground for surveillance technologies developed by both domestic and international actors. Weak regulatory frameworks, limited public oversight, and institutional fragility create ideal conditions for the experimentation and deployment of invasive digital tools. From facial recognition systems in public spaces to predictive policing algorithms and mass data collection initiatives, various technologies have been implemented with minimal transparency or accountability.

These deployments often occur in marginalized urban areas, effectively turning vulnerable populations into subjects of technological experimentation without informed consent or legal safeguards. This dynamic is further reinforced by partnerships between the Brazilian state and private tech companies, which often provide surveillance infrastructure in exchange for access to vast amounts of personal data. Such collaborations blur the lines between public interest

[16] Castells (1996) understands that the dimensions of society, grounded in local histories and traditions, are overshadowed by a cold, calculative logic that defines what is considered valuable or worth pursuing in the digital age. The reliance on technological systems as the primary mode of organizing and governing these economies leads to the erosion of traditional forms of sociality and governance.

[17] According to Brown (2015), *Neoliberal rationality* is characterized by profit-driven expansion and commodification, devalues human life. In Southern Neoliberal Economies, technology can serve as a mechanism of societal control, rooted in racial inequalities and structural inequality.

[18] According to Mbembe (2021), Digital rationality can be understood as imposition of systems of control, efficiency, and data-driven decision-making, against the local cultural, economic, and political contexts on any semi-peripheral economies.

and corporate profit, allowing experimental systems to operate under the guise of public security or digital modernization. The lack of robust cybersecurity defenses and independent regulatory institutions facilitates this asymmetry, enabling powerful actors to pilot and refine surveillance strategies with little regard for civil liberties. As a result, Brazil not only inherits the consequences of this unchecked experimentation, such as increased social control, data breaches, and discriminatory policing, but also contributes to the normalization of these practices in the global digital security industry.

Within this context, updating the notion of *coloniality*[19] makes it clear just how the exploration of Brazil's colonial[20] heritage is entrenched with patterns of violent governance, economic exploitation, and racial subjugation that continue to persist in the *modern era*. The persistence of *coloniality* is evident in the continuous exploitation and marginalization of *the colored* and *the poor* that perpetuates systemic exclusion and *dehumanization*. With the proliferation of digital technologies and the pressures of digital modernization, I testify to the rise of a *violent model of development* that entrenches the *status quo of exclusion* and amplifies its existing social/historical social inequalities.

The arrival of new technologies tends to *reinforce* rather than *disrupt* existing power dynamics, deepening societal divisions and creating further barriers for those already marginalized. This reliance on technology as the primary mode of organizing and governing leads to the *erosion of traditional forms* of sociality and governance, further entrenching the inequities embedded in Brazil´s social fabric. *Technolatry* reflects a global technological imperative, in which the values and priorities of core economies are imposed on the Global

[19] For Quijano (2000), *coloniality* refers to the enduring patterns of power that emerged from colonialism but continue to shape global systems, identities, and social hierarchies long after the colonial administrations ended. These patterns are maintained through the intersection of race, labor, knowledge, and authority, forming a *coloniality of power* that underpins modern societal structures.

[20] According to Bora (2024a), in Brazil, *coloniality* was manifested through various forms, such as, violent governance, religious takeover, cultural subjugation, economic exploitation, and racial genocide. Dominant powers exploited the colonies´ resources as well as the man/labor and its markets. Modern Brazilian society is a complex socio-legal paradigm that reflects the contradictory coexistence of modernity and coloniality. A democratic and multicultural nation that also reproduces and perpetuates the colonial patterns of power in its institutions.

South, leading to a paradigm where local communities, cultures, and economies are increasingly subordinated to a *global digital logic* [21].

This dynamic is further compounded by *systemic corruption*, as officials and institutions increasingly leverage digital transactions. *Corruption* becomes not only more concealed but also more efficient and far-reaching in the digital age, enabling elite actors to consolidate power while evading accountability. The opacity offered by blockchain technologies and the lack of stringent enforcement mechanisms make these digital avenues particularly attractive for laundering public funds, embezzlement, and illicit campaign financing.

In low-income communities, where education systems often fail to provide even basic digital skills, individuals are more likely to fall victim to deceptive emails, fake websites, and malicious software. Cybercriminals exploit this gap by targeting unsuspecting users with fraudulent banking notifications or social benefit scams, particularly those tied to government assistance programs like *Bolsa Família* [22] and other welfare aids. These attacks not only result in personal financial loss but also foster deep *mistrust* in public digital infrastructure, further alienating marginalized groups from digital engagement and reinforcing their systemic exclusion.

Additionally, small businesses, informal workers, and independent service providers, who often rely on unsecure networks and outdated devices, are increasingly targeted by *ransomware attacks* and *online extortion* schemes. In Brazil, a country with a large informal economy, many of these victims have no access to legal recourse or cybersecurity support, leaving them to absorb the full impact of the attack or, worse, pay ransoms to continue operating. As a result, traditional cybercrime in Brazil functions not just as a technical threat

[21] The integration of *digital rationality* into these economies, far from being a neutral or purely progressive force, often reveals the harsh realities of global capitalist expansion, where the peripheral becomes more entangled in the forces of global technology, without gaining the means to truly shape its own future (Mbembe, 2023).

[22] *Bolsa Família* is a social welfare program in Brazil designed to reduce poverty and inequality by providing direct cash transfers to low-income families. Implemented in 2003, the program targets families living in poverty or extreme poverty, with benefits conditional on meeting specific requirements such as ensuring children attend school and receive vaccinations. The goal is not only to alleviate immediate financial hardship but also to break the cycle of poverty by investing in education and health. Bolsa Família is internationally recognized for its role in improving social indicators and promoting social inclusion in Brazil.

but as a structural force that widens economic disparities, undermines trust in digital systems, and amplifies the marginalization of those already on the socio-economic periphery.

Simultaneously, militias and drug factions have adapted rapidly to the digital terrain, exploiting the same technologies to entrench their influence and control. These groups utilize encrypted messaging apps to coordinate criminal operations and evade law enforcement, while social media platforms serve as powerful tools for psychological warfare, broadcasting acts of violence, issuing threats, and promoting a *culture of fear* to maintain dominance over local populations. Their strategic use of digital communication blurs the lines between organized crime and political propaganda, manipulating public perception and normalizing violence as a form of governance. Moreover, these non-state actors increasingly employ surveillance technologies such as closed-circuit cameras, facial recognition systems, and drones to establish territorial oversight and enforce their own rules. This form of *techno-sovereignty* creates an alternative governance structure, one that rivals and often surpasses the reach and effectiveness of official state institutions in marginalized areas. In doing so, these factions institutionalize a *shadow digital state* that further erodes public trust, deepens the fragmentation of state authority, and exacerbates existing inequalities in security, access, and rights.

Recognizing these dynamics is crucial to avoid framing technology as the origin of dysfunction, rather than a medium through which existing inequalities are reinforced or contested.

## 2. The endemic proliferation of Cybercrime and Case Studies of *Modern Brazil*

In Brazil, the rise of cybercrime is inseparable from the philosophical underpinnings of *Postcolonial heritage* and *Technolatry*. As a result, its proliferation can be seen as a natural consequence of a world that places technological determinism at the center of its foundational existence, pushing aside the ethical, political, and social implications of unregulated technological expansion (Fuchs, 2017). Today, there are new avenues for exploitation and manipulation, where the rules and understandings of the *physical world* no longer apply. The detachment from traditional forms of governance, the erosion of privacy,

and the reduction of individuals to *data* are all symptoms that indicate that Brazil is in fact living the *digital brutalist experience*.

The increasing reliance on digital technologies, particularly in financial and governmental sectors, exposes Brazilian society to the risks associated with *technolatry*. The convergence of digital transformation, criminal activity, and socio-political dynamics illustrates the complex and multifaceted nature of cybercrime in Brazil (Nascimento, 2018). As it has been noted, the rise of digital crime, pronounced in Brazil, is due to its position as a developing economy with relatively weak cybersecurity measures, lack of adequate regulatory frameworks, and with widespread misuse of digital platforms, making Brazil an ideal target for cybercriminals (Moreira & Amado, 2019). The Brazilian government's response has been reactive rather than proactive, further entrenching the digital and society's inequality. And as it goes, the country's cybersecurity infrastructure remains underdeveloped, and it continues to face struggles in implementing effective regulations against digital crimes (Nascimento, 2018).

The increasing reliance on digital technologies, particularly in financial and governmental sectors, exposes Brazilian society to the risks associated with *technolatry*. The convergence of digital transformation, criminal activity, and socio-political dynamics illustrates the complex and multifaceted nature of cybercrime in Brazil (Nascimento, 2018).

According to the United Nations (2010), individuals and criminal groups operating in the *Cyberspace*[23] are believed to be more flexible compared to traditional perpetrators of *crimes*. This understanding can be extended to their motivations, organizational structures, and even towards the types of rewards these individuals and groups seek out. *Cybercriminals* do not require control over a geographical territory, need fewer personal contacts, and need less

[23] Graham (1998) argues that traditional spatial metaphors, rooted in Cartesian geometry, are insufficient for understanding the complexities of the *Cyberspace*. Instead, he advocates for a more relational and dynamic approach to conceptualizing it, one that acknowledges its multidimensionality, fluidity, and embeddedness within social and cultural contexts. He understands that "the technologies of media, computing and telecommunications converge and integrate; as equipment and transmission costs plummet to become virtually distance independent; and as broadband integrated networks start to mediate all forms of entertainment, social interaction, cultural experience, economic transaction and the labor process, distance effectively dies as a constraint on social, economic and cultural life" (p. 13).

enforcement of physical discipline and coercion between criminals (Wall, 2007). Tropina (2024) understands that cybercrime has moved away from individual, fragmented activities to a model of crime that *mimics* the modern *corporate business* (Tropina, 2024). Digital crimes are being reorganized through the formation of new groups of criminals that operate only in the *Cyberspace*[24].

In this context, *Online forums*[25] serve as a vital space for recruiting individuals that seek contact with the underground economy, since they facilitate cooperation within and between groups, enabling offenders to even work together on specific projects. *Darkweb Marketplaces*[26]*,* are also fundamental for this dissemination and represent the platform for advertising, learning, and information-sharing. *Darkweb Marketplaces* facilitate transactions between businesses in the criminal underworld, helping cybercriminals buy and sell services, tools, and stolen data. They provide a platform for cybercriminals to connect and conduct business transactions in a manner similar to *legitimate B2B platforms (*e.g., Alibaba, Shoppee, etc.). According to Tropina (2024), the data traded on these shadow platforms carries its own monetary value, representing an illicit commodity that is both intangible and easily transferable across borders.

Bent-Izthak (2008) highlights that, in the present day, cybercriminals utilize schemes similar to legitimate B2B (business-to-business) operations, referred to as C2C (criminal-to-criminal). These operations often involve a supply chain of services and products, with cybercriminals

[24] In this sense, all information becomes accessible *everywhere* and *anywhere*. *Human life* becomes liberated from the constraints of space and frictional effects of distance. Everything happens, all the time, at the same time, anything is possible. "The boundaries between humans and machines become ever more blurred, permeable and *cyborgian*" (Graham, 1998, p.15).

[25] These *Online forums* demonstrate how online platforms facilitate collaboration and cooperation within the digital *shadow* economy, enabling offenders to organize and work together on specific projects, ranging from hacking and fraud to the distribution of pirated software and stolen data.

[26] According to Martin (2014), *DarkWeb Marketplaces* are hidden platforms within the Dark Web that facilitate the buying and selling of illegal or illicit goods and services, such as drugs, weapons, counterfeit documents, and hacking tools. These marketplaces operate anonymously using technologies like Tor or I2P and often use cryptocurrencies to ensure untraceable transactions. They rely on reputation systems, escrow services, and encryption to build trust among users while evading law enforcement. Despite their illegality, these marketplaces have a significant impact on global criminal networks, showcasing the intersection of technology and illicit economies.

developing or acquiring tools and services to facilitate various stages of an attack[27]. This network spans a wide range of expertise that can go from *malware development*, *hacking tools*, *data theft*, *money laundering*, developing *exploitation tools* (such as exploits[28] and botnets); *tools to attack commercial databases* [29] (phishing, pharming, malware); *Crimeware*[30] (tools such as Viruses, Trojans, and keyloggers), and *other services* (malicious code-writing, crimeware distribution, lease of networks), all of which offer criminal groups the flexibility of controlling, stealing, and trading data. *Ransomware* attacks and other forms of cybercriminal activity have become ubiquitous in the digital age and represent new manifestations of cybercrime in Brazil.

*Ransomware* is a particularly malicious form of cybercrime that involves encrypting a victim's data and demanding payment for its release. This form of cybercrime is both an economic and psychological attack, as it places individuals and businesses under duress, forcing them to choose between paying the ransom or losing their valuable data. The proliferation of *ransomware* attacks can be seen as a reflection of *lack of trust*[31] in Brazilian formal institutions, and criminal organizations may see it as a more effective way of achieving financial gain when compared to traditional forms of crime. The decentralized nature of *ransomware* networks allows for decentralized control over criminal activities, which appeals to groups that operate

[27] Inside a criminal organization, one might work in coding a malware, another in distributing it, another in collecting the crime profits. Each component operates independently but collaborates to achieve the overall goal, similar to how legitimate businesses collaborate within a supply chain (Ben-Itzhak, 2008)

[28] According to Bora (2024b) *Exploitation tools* are used to identify and exploit vulnerabilities in software or systems. Exploits are specifically crafted to take advantage of weaknesses in software or network protocols, while *botnets* consist of networks of compromised computers controlled by a single entity for malicious purposes.

[29] *Tools to attack commercial databases* encompasses various techniques aimed at compromising commercial databases for illegal purposes. Examples include *Phishing*, which involves fraudulent attempts to obtain sensitive information such as usernames, passwords, and credit card details by posing as a trustworthy entity, and *Pharming* which redirects website traffic to fraudulent websites for the purpose of stealing personal information.

[30] Bora (2024c) understands that *crimewares* refers to a category of virus based malicious software designed to carry out criminal activities, such as *Viruses*, *Trojans*, and *Keyloggers*. *Viruses* are self-replicating programs that spread by attaching themselves to other files or programs, while *Trojans* disguise themselves as legitimate software to trick users into installing them, and *keyloggers* record keystrokes to capture sensitive information like passwords and credit card numbers.

[31] Giddens (1991) discusses how *trust* in formal institutions (such as governments and financial systems) is crucial in modern societies. When such *trust* erodes, individuals and groups may seek alternative, often illicit, ways to achieve their goals, this way the rise of ransomware attacks in Brazil can be seen as a symptom of weakened *institutional trust*.

outside the boundaries of the state's authority (Castells, 1996; Van Dijlk, 2020; Melo, 2019; Maras, 2019).

Maras (2019) understands that *Deepfakes*, similarly to ransomware, also represents a new frontier of cybercriminal activity. By leveraging advanced artificial intelligence, cybercriminals can create convincing but entirely fictitious videos, audio clips, or images that manipulate public opinion or defraud individuals. The ability to create *hyper-realistic digital identities* without the constraints of physical reality exposes the fragile boundary between the *real* and the *virtual* (Baudrillard, 1994). These crimes are emblematic of the broader trends of *symbolic manipulation* and *technological subjugation* (Castells, 1996 Quijano, 2000; Mbembe, 2021. They highlight the vulnerability of contemporary society to digital exploitation, as the very fabric of truth and reality can be digitally *reconstructed*, *manipulated*, and *weaponized* to criminal ends (Maras, 2019).

Brazil sits at the intersection of global technological integration and local socio-economic challenges; its *status* allows it to both benefit from technological advancements and fall victim to their exploitations. In the Brazilian paradigm, there is an uneven development, and integration into the global market has resulted in this increased vulnerability to external shocks and opportunities for growth driven by *technology* (Melo, 2019). In Brazil, *Cybercrime* reflects a global trend toward increasingly sophisticated and organized digital criminal activities[32], becoming clear that the structural conditions of cybercrime in Brazil[33] are expansive and well-coordinated illegal operations. In 2014, it was ranked number one by

[32] According to CNN Brazil, the operation, called *Operação Guardião*, conducted by Pará's Civil Police with support from São Paulo's Civil Police, arrested 32 individuals involved in cybercrimes. The targets included criminal networks responsible for scams like fake vehicle auctions, fraud on sales platforms, WhatsApp account hacking, and crimes against children, such as child pornography and cyberbullying. Authorities carried out 103 search warrants across 12 municipalities in São Paulo. The schemes mainly victimized people in Pará and other Brazilian regions. Accessed in 29/12/2024, CNN Brasil. (2024). *Police operation against cybercrimes arrests 32 people in São Paulo*. Available at: https://www.cnnbrasil.com.br/nacional/operacao-policial-contra-crimes-ciberneticos-prende-32-pessoas-em-sao-paulo/

[33] Messaging platforms in Brazil are essential tools for Brazilian cybercriminals. These mainstream messaging apps operate in specialized dark web marketplaces, serving, as we know, as hubs for the sale of stolen data, hacking tools, and other illicit services. And according to Security Affairs (2014), the existence of such localized platforms underscores the adaptability and market-focused strategies of Brazilian cybercriminals, enabling them to thrive in a rapidly evolving digital landscape.

*Kaspersky Lab* for banking malware attacks, with nearly 300,000 compromised users. The persistence of such crimes highlights vulnerabilities in financial systems and the pressing need for enhanced cybersecurity measures. Brazil has been a hotspot for several types of cybercrimes[34] [35]; in 2022, according to IBM (2024) the average cost of a data breach for Brazilian companies was approximately US$4.35 million. The country consistently ranks among the top countries globally for cybercrime, particularly in banking fraud and financial malware. A recent report by Symantec (2023), a cyber-security company, places Brazil in third place globally in terms of sources of *malware*, *bots*, *spam*, and *phishing attacks*, with 5.4% of global threat detections originating in the country. The number of Brazilians using the internet has increased from less than 3% of the population in 2000, to more than 66% in 2016[36].

According to Security Affairs (2014), the Brazilian underground, in relation to other major epicenters of cybercrime such as Russia, China, and the USA, is *distinct* due to the availability of training services. These services are often accessible to individuals with minimal experience in cybercrime, providing a pathway for new recruits to gain expertise and participate in illegal activities.

[34] According to the Igarapé Institute (2018), during the 2016 Olympics in Brazil, ATMs, restaurants and shopping venues, were the main targets for *credit card skimming*, *cloning scams*, and more sophisticated crime techniques such as *radio frequency interception* (RFI). The targets of cybercrime in Brazil are not limited to government agencies and large organizations. Regular citizens, visitors, and small and medium-sized businesses are also frequently targeted. The Brazilian authorities reported more than 100,000 instances of internet related fraud in 2016. According to the Brazilian Federation of Banks (*Federação Brasileira de Bancos: Febraban*), more than 50% of all financial transactions in Brazil are made using internet-connected devices, generating significant scope for cyber theft.

[35] According to Security Affairs (2014), Brazil has a lack of concrete laws and limited law enforcement agency resources that address cybercrime in the country. Additionally, the technological and consumer landscape in Brazil, which has a *50% Internet penetration rate*, and a *69% credit card penetration rate,* has made the country all too appealing for cybercriminals. However, another factor may have also contributed to Brazilian cybercrime: the existence of a flexible underground market with different offerings, ranging from banking Trojan development to online fraud training.

[36] In line with this, the number of reported cyberattacks has also climbed sharply, from fewer than 10,000 per year when Brazil first began keeping track in 1999, to a peak of more than one million reported attacks in 2014, the year that Brazil hosted the FIFA World Cup. More than half of all reported attacks in 2015 and 2016 originated inside Brazil, followed by attacks from within China and the United States.

We can see an ecosystem that helps proliferate illicit activities, and the most used primary venues for this proliferation are the messaging platforms, such as WhatsApp and Telegram[37], the dark web marketplaces. The Brazilian underground ecosystem is thus considered a prominent market for *cybercriminal apprentices*, where newcomers can quickly learn, practice and instruct illicit activities. In contrast to other regions, where expertise is typically more centralized and difficult to attain, like Russia or China, the Brazilian ecosystem offers a more open environment for aspiring cybercriminals to hone their skills, making it a key player in the global cybercrime landscape. I understand that The Brazilian cyber criminals seem to be more ruthless in the use of media platforms like Facebook, YouTube, Twitter, Skype, and WhatsApp, differently from Russian and Chinese players that usually hide in the *Deep Web* and use tools that ordinary users do not.

> "What distinguishes the Brazilian underground from others is the fact that it also offers training services for cybercriminal wannabes," according to the whitepaper. Cybercriminals in Brazil particularly offer FUD (fully undetectable) *crypter* programming and fraud training by selling *how-to* videos and providing support services via Skype. Anyone who is Internet savvy and has basic computing knowledge and skill can avail of training services to become cybercriminals. How-to videos and forums where they can exchange information with peers abound underground. Several trainers offer services as well. They even offer support when training ends" (Security Affairs, 2014, p.10)

As it can be seen, the statement highlights a unique characteristic of the Brazilian underground cybercriminal ecosystem, its focus on education and accessibility for aspiring cybercriminals. It is the *democratization of cybercrime*, where barriers to entry are reduced by the availability of resources. By lowering the technical expertise required, these services enable individuals with basic computing knowledge to *participate*. The use of mainstream platforms for direct

[37] According to CNN Brazil (2024), a report by *SafeNet* reveals that over 1 million Brazilians are involved in groups linked to *child pornography*, mainly on Telegram. The organization identified active links facilitating these crimes, with some communities hosting over 1.25 million users. The findings were submitted to Brazil's Federal Public Ministry to support investigations. Telegram, while claiming to use AI and moderators to fight such content, faces criticism due to the alarming scale of the issue, highlighting challenges in combating this crime. Accessed in 29/12/2024 avalible in : CNN Brasil. (2024). *Um milhão de brasileiros participam de grupos com pornografia infantil, diz relatório*. Retrieved from https://www.cnnbrasil.com.br. (One million Brazilians are part of groups sharing child pornography, according to report).

support is a telling sign of how accessible these illicit activities have become, blurring the line between professionalized crime and opportunistic ventures. This accessibility is particularly concerning as it creates a pipeline for continuous growth of cybercriminal networks.

By embedding training services within their operations, Brazilian cybercriminals are not just conducting crimes but actively investing in the development of future perpetrators. This also contributes to the perpetuation of advanced threats globally, as the techniques and tools honed in this underground ecosystem are likely to spread across international boundaries.

## Conclusion

The concept of *digital brutalism*, rooted in Achille Mbembe's theoretical framework, provides a powerful analytical lens for understanding how technological systems, imported and uncritically adopted, exacerbate existing inequalities and foster exploitative environments in Brazil. Algorithmic structures dictate parameters of visibility and engagement. These digital spaces amplify certain emotions and embed them with *traceability* and *predictability* of human behavior to be weaponized against them.

In my body of work, *Modern Brazil*, served as a case study to examine the entangled relationships between technology, socio-economic asymmetries and colonial historical legacies. *Cybercrime in Brazil* is a pressing issue with far-reaching implications that connects with themes of *colonial heritage*, *economic stability* and *public security*. The intersection with *technolatry* and the rampant growth of cybercrimes show us that there is an urgent need for a multifaceted approach to address this complex social and technological phenomenon. However, it is equally crucial to underline the importance of a *decolonial consciousness* in these initiatives.

I believe that sociological understandings of the historical and structural inequalities that shape Brazil's socio-digital landscape are essential to address how power imbalances and systemic exclusions continue to influence technology and cybercrime. In Brazil, these historical legacies have been magnified, with marginalized groups facing greater vulnerability to cybercrimes, either as *perpetrators* or *victims*. This paradigm is compounded by the *digital*

*divide*, where disadvantaged communities struggle with limited access to technology and cybersecurity knowledge, leaving them more susceptible to cybercriminal activities.

Brazil lives a *digital brutalist experience* and the detachment from traditional regulatory frameworks, the lack of robust cybersecurity measures, and the widespread use of unsecured digital platforms make it an ideal target for cybercriminals. And this vulnerability is also compounded by a reactive governmental approach that often lags behind the pace of *technological advancement*, further entrenching societal inequalities and exposing marginalized populations to heightened risks. Ultimately, the convergence of digital transformation, criminal activity, and socio-political dynamics in Brazil is an understudied multifaceted phenomenon that shows us that *technological innovation*, when uncritically adopted within this context of inequality, becomes both a *tool of power* and a *mechanism for systemic exploitation*.

I tried to highlight that, in Brazil, proactive governance and robust cybersecurity infrastructure is not enough to change the fundamental conceptuality and beliefs intertwined *in* and *through* technology. I believe that incorporating *decolonial consciousness* into the approach of Cybercrime in Brazil helps us recognize the existence of deep-rooted social issues and understand how they intertwine with the rise of digital technologies. It requires addressing not only the technical aspects of cybercrime but also the socio-economic inequalities that exacerbate it. By doing so, initiatives aimed at combating cybercrime could have a chance of becoming more inclusive, equitable, and effective, consequently ensuring that all digital ecosystems are accessible, secure, and just for all, regardless of socio-economic background. This framework would enable Brazil to confront cybercrimes while also addressing the historical imbalances that continue to affect its *digital future*.

In this sense, *enhanced international cooperation* is essential, the transnational nature of cybercrime demands stronger alliances between Brazil and global law enforcement agencies to share best practices, intelligence, and resources, through which Brazil can bolster its ability to combat cyber threats that transcend national borders, fostering a more secure digital environment. Alongside these efforts, public awareness campaigns play a vital role in

reducing individual and systemic vulnerabilities. Educating citizens and organizations about cybercrime risks and preventive measures can foster a culture of digital responsibility, encouraging safer online practices that mitigate potential threats. Ultimately, addressing these challenges requires a holistic strategy that integrates technological advancements, international collaboration, and sociological insights. By doing so, Brazil can not only confront the proliferation of cybercrimes but also navigate the complexities of the digital era with greater resilience and equity in the digital ecosystem.

I share Mbembe's perspective and also defend a new *global consciousness*, one that emphasizes repair, solidarity, and the reconstruction of communities in the face of all this overwhelming adversity. A vision of *new politics* that is not simply about *resistance* but about the *creation* of new ways for living beings *to live*. Ways to flourish our existence in the world, ways to provide mutual aid, and acquire ecological responsibility, but above all, recognize our *shared humanity*. The *scars of history* are not erased but must be woven into a tapestry of *renewal*. History should not be forgotten but rather acknowledged and used as part of positive transformation.

A *new consciousness* must sing across borders; its rhythm should resonate justice, and its melody should pulse in the veins of every community in *Latin America* and across the *Global South.* We should envision a reckoning of this world, and in its ruins, transform the future into a fertile ground for *collective growth*.

Curing political and historical injustice is a complex task that goes beyond structures and human eyes; it should reach the *soul* of individuals and societies, help us *cultivate* and celebrate a positive *interconnectedness* among us through the proliferation of new *human springs*.

The *Tupi-Guarani* are a group of indigenous people that belong to the *Tupi* linguistic branch, one of the main indigenous language families in *South America*. They believe that healing the *earth* is a *spiritual* and ethical act, recognizing the intrinsic connection between ecological well-being and the collective health of *humanity*. They understand that by caring for the soil,

waters, and ecosystems, we also care for our *essence*, restoring a lost balance between *nature and our existential condition*. This perspective resonates and views the earth as a *living organism*, where the repair of the external world directly reflects inner *harmony*, awakening a consciousness of shared responsibility and profound reconnection.

We conclude with the following *reflection*, as expressed in Tupi-Guarani:

*Ñandé jereko jevy yvy rehe ha ñandéve voi.*

*Tataendy ñandé rupa ha ñande kuarasy ombopohé ñande ayvu.*

Which translates to:

"Let us reconnect with the world and, with it, ourselves."

"Let us heal the *earth*, and by doing so, heal our *soul*."

## Referências bibliográficas

AHMED, S. (2004), *The Cultural Politics of Emotion*, Edinburgh, Edinburgh University Press.

BORA, S. S. M. (2020), "Understanding neoliberalism through racial discrimination: An approach to the mass incarceration problem in Brazilian prison system", *Revista Debates Insubmissos*, Pernambuco Federal University (UFPE). Ano 3, 3 (10), mai. /ago. ISSN 2595-2803.

BORA, S. (2024a). *Poscolonialismo y selectividad racial en el sistema punitivo brasileño: Un análisis criminológico del paradigma del encarcelamiento masivo*. Crítica Penal y Poder, *(27)*. https://doi.org/10.1344/cpyp.2024.27.47093

_____(2024b). *IaaS Cloud Model Security Issues: Vulnerabilities and the most common attacks*. *RECiC Revista de Ciência da Computação*, ISSN 2596-2701, 1 jun. 2024.

_____(2024c). *Fundamentals of intrusion detection and prevention system in cloud environments*. *Revista Processando o Saber*, 17 abr. 2024.

BAUDRILLARD, J. (1993), *The transparency of evil: Essays on extreme phenomena* (J. Benedict, Trans.), Verso. (Original work published 1990)

_____ (1994), *Simulacra and simulation* (S. F. Glaser, Trans.), University of Michigan Press. (Original work published 1981)

BENT-IZTHAK, Y. (2008), "Cybercrime and the Challenges of International Cooperation", In: Tatiana Tropina, Cian Callanan (Eds.), *Organized Crime in Cyberspace: An Analysis of Cybercrime and Measures to Combat It*, Bielefeld: transcript Verlag, p. 47–62.

BAUMAN, Z. (1999), *Liquid modernity*, Cambridge, Polity Press.

_____ (2003), *Liquid love: On the frailty of human bonds,* Cambridge, Polity Press.

_____(2006), *Liquid fear*,Cambridge, Polity Press.

BAUMAN, Z., (2013), *Liquid surveillance*: A conversation, Cambridge, Polity Press.

BOYER, C. (2019), *Brutalism: The power of architecture*, New Haven, Yale University Press.

BROWN, W. (2015), *Undoing the demos*: Neoliberalism's stealth revolution, Cambridge, Zone Books.

CASTELLS, M. (1996), *The rise of the network society* (Vol. 1), Oxford, Blackwell Publishers.

FUCHS, C. (2017). *Social media: A critical introduction* (2nd ed.), SAGE Publications.

GOLDHAGEN, S. W., & LEGAULT, S. (2000), *Anxious Modernisms: Experimentation in Postwar Architectural Culture*, Cambridge, MIT Press.

GRAHAM, S. (1998), "The end of geography or the explosion of place? Conceptualizing space, place and information technology"*, Progress in Human Geography*, 22(2), 165–185.

IGARAPÉ INSTITUTE. (2018). *Brazil struggles with effective cyber-crime response.* Retrieved December 29, 2024, from https://igarape.org.br/en/brazil-struggles-with-effective-cyber-crime-response.

IBM Security (2024). *Cost of a Data Breach Report 2024*. Cambridge, MA: IBM Corporation, Disponível em: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs. Acesso em: 4 jun. 2025.

LIPOVETSKY, G. (2005). *A era do vazio: Ensaio sobre o individualismo contemporâneo* (M. P. Rouanet, Trad.), São Paulo, Manole. (Obra original publicada em 1983).

MARAS, M. H. (2019), "Deepfakes and the coming infocalypse: A survey of the state of the art and future challenges", *International Journal of Cybersecurity and Digital Forensics*, 2(1), 41–61.

MARTIN, J. (2014), *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*, Londres, Palgrave Macmillan.

MBEMBE, A. (2019), *Necropolitics*, North Carolina, Duke University Press.

MBEMBE, A. (2021), *Brutalismo*, São Paulo: n-1 edições.

MIGNOLO, W**.** (2017) Colonialidade: o lado mais escuro da modernidade. Tradução de Marco Oliveira. *Revista Brasileira de Ciências Sociais*, São Paulo, 32 (94), e329402, Disponível em: https://www.scielo.br/j/rbcsoc/a/nKwQNPrx5Zr3yrMjh7tCZVk/?lang=pt. Acesso em: 4 jun. 2025.

MELO, M. A. (2019),"Digital transformation and development in Latin America: Beyond dependency theory", *Latin American Politics and Society*, 61(3), 1–23.

MOREIRA, R., & AMADO, G. (2019). *The rise of digital crime in Brazil: The vulnerabilities of a developing economy.* Journal of Cybersecurity and Digital Justice, 4(2), 123–135. https://doi.org/10.1000/jcdi.2019.004

NASCIMENTO, L. (2018), "Cybersecurity in Brazil: A reactive approach to digital crime", *Brazilian Journal of Technology and Law*, 12(1), 45–58. https://doi.org/10.1000/bjtl.2018.012

QUIJANO, A. (2000), "Coloniality of Power, Eurocentrism, and Latin America", *Nepantla: Views from South*, 1(3), 533–580.

SIMMEL, G. *The Metropolis and Mental Life*. In: Simmel, G. *The Sociology of Georg Simmel*. Translated and edited by Kurt H. Wolff. New York: Free Press, 1950.

SPIVAK, G. C. (1999), *A critique of postcolonial reason: Toward a history of the vanishing present*, Cambridge: Harvard University Press.

SECURITY AFFAIRS (2014), *Brazilian underground cyber market*. Retrieved from https://securityaffairs.com/30350/cyber-crime/brazilian-underground-cyber-market.html?utm_source=chatgpt.com

SYMANTEC (2023), *Cybersecurity threat report*, Symantec. Retrieved from https://www.symantec.com

TROPINA, T. (2024), "Organized crime in cyberspace", In Heinrich-Böll-Stiftung & R. Schönenberg (Eds.), *Transnational organized crime: Analyses of a global challenge to*

*democracy* (pp. 85–104), Bielefeld, Transcript Verlag. Retrieved from https://www.jstor.org/stable/j.ctv1fxh0d.8

UNITED NATIONS (2010), *Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime,* Twelfth United Nations Congress on Crime Prevention and Criminal Justice (Working Paper V.10-50382). Salvador, Brazil, April 12–19.

VAN DIJK, Jan A. G. M. (2020), *The Digital Divide*, Cambridge: Polity Press.

WALL, D. S. (2007), *Cybercrime: The transformation of crime in the information age,* Cambridge, Polity Press.

WALLERSTEIN, I. (2004), *World-systems analysis: An introduction,* North Carolina, Duke University Press.

ZUBOFF, S. (2019), *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, New York, PublicAffairs.

**Siddharth S.M. Bora.**

PhD Candidate at the University of Coimbra, Portugal. Faculty of Economics, Department of Sociology. Rua Doutor Henrique Seco, n.08, 3000-145 Coimbra. ORCID ID: 0000-0002-3908-3101.
E-mail: sbora08@gmail.com

BORA, Siddharth S.M. (2025),
"Technolatry and Virtual Emotions in the Era of Digital Brutalism: Understanding the proliferation of Cybercrimes in Modern Brazil",
*Sociologia: Revista da Faculdade de Letras da Universidade do Porto,* Vol. LI, pp. 95 - 124
DOI: https://doi.org/10.21747/08723419/soc51a4