pensar
Revista de Ciências Jurídicas
Universidade de Fortaleza
e-ISSN:2317-2150
10.5020/2317-2150.2024.16823

Criminality, Viligiance and Biometric Behavioral Recognition Technologies*

Criminalidade, Vigilância e Tecnologias de Reconhecimento Biométrico Comportamental

Criminalidad, Vigilancia y Tecnología de Reconocimiento Biométrico de Comportamiento

Alejandro Knaesel Arrabal[**]
Lenice Kelner[***]
Leandro Felix da Silva[****]

Abstract

This work offers resources for the use of biometric recognition technologies, whether public in relation to activities mediated by information technology, in monitoring in private environments. As a theoretical framework (place of speech) it considers Critical Criminology as the science that explains the operation and real functions of the penal system, which can offer elements to guide the use of information technologies in the field. Developed using the hypothetical deductive method and based on a bibliographical review, the work is structured into three units. The first explores aspects of corporeality as an expressive dimension of individual personality. The second part addresses the general technical aspects of behavioral biometrics. Finally, the third technology unit to respect the use of this fin technology of surveillance in the penal system. Contributions from the study indicate that digital surveillance devices do not distance themselves from punitive logic; on the contrary, they emerge to compose the punishment diagram, configuring an era of social control technology as criminal policy.

Keywords: Behavioral Biometrics; surveillance; Critical Criminology.

Resumo

Este trabalho oferece um panorama sobre tendências, benefícios e limitações a respeito do potencial emprego de tecnologias de reconhecimento biométrico comportamental como incremento do combate ao crime, seja em relação as atividades delitivas mediadas por tecnologia da informação, seja no monitoramento de pessoas em ambientes públicos e privados. A título de marco teórico (lugar da fala) considera-se a "Criminologia Crítica" por ser a ciência que procura explicar

[1] Artigo traduzido por meio de Inteligência Artificial.

** PhD in Public Law from the Graduate Program in Law at the University of Vale dos Sinos – UNISINOS (2017). Master's degree in Legal Sciences from the University of Vale do Itajaí – UNIVALI (2003). Specialist in Administrative Law from the Regional University of Blumenau – FURB (1996). Professor and researcher of the Master's Programs in Law (PPGD) and Administration (PPGAd) at FURB. Leader of the research group Law, Technology and Innovation – DTIn (CNPQ-FURB). Vice-leader of the SINJUS Research Group – Society, Institutions and Justice (CNPq-FURB).

*** PhD in Public Law from the Graduate Program in Law at the University of Vale dos Sinos – UNISINOS. Postdoctoral internship in Criminology from the Graduate Program in Law of the State University of Rio de Janeiro – UERJ Master's degree in Legal Sciences from the University of Vale do Itajaí – UNIVAL. Specialist in Criminal Law and Criminal Procedure from the Regional University of Blumenau ? FURB. Specialist in Civil Law from the Regional University of Blumenau – FURB. Permanent Professor of the Master's Program in Law and Undergraduate Program in Law at the Regional University of Blumenau – FURB.

**** Specialist in Computer Forensics and Digital Forensics from IPOG and Database from Claretiano. Technologist in Internet Systems from FATESM and Bachelor of Laws from the Regional University of Blumenau – FURB. Information Technology Analyst at the Federal Institute of Santa Catarina, he currently holds the position of Data Officer (DPO). Computer Expert and Technical Assistant.

a operacionalidade e as reais funções do sistema penal, o que pode oferecer elementos para balizar o emprego de tecnologias de informação no campo. Realizado a partir de revisão bibliográfica, o trabalho encontra-se estruturado em três unidades. A primeira explora aspectos a respeito da corporeidade como dimensão expressiva da personalidade individual. Na segunda parte abordam-se aspectos técnicos gerais sobre a biometria comportamental. Por fim, a terceira unidade propõe reflexões a respeito do emprego dessa tecnologia para fins de vigilância no sistema penal.

Palavras-chave: *Biometria comportamental; Vigilância; Criminologia crítica*

Resumen

Este trabajo ofrece un panorama sobre tendencias, beneficios y limitaciones a respecto del potencial empleo de tecnologías de reconocimiento biométrico de comportamiento como incremento para el combate al crimen, sea en relación a las actividades delictivas mediadas por tecnología de la información, sea en el monitoreo de personas en ambientes públicos y privados. A modo de marco teórico (lugar del habla) se adopta la criminología crítica por ser la episteme que busca explicar la operacionalidad y las reales funciones del sistema penal, lo que puede ofrecer elementos para balizar el empleo de las tecnologías de la información en el campo. Desarrollado por el método hipotético-deductivo y a partir de revisión bibliográfica, el trabajo se encuentra estructurado en tres unidades. La primera explora aspectos a respecto de la corporeidad como dimensión expresiva de la personalidad individual. En la segunda parte se enfocan aspectos técnicos generales sobre la biometría de comportamiento. Por fin, la tercera unidad propone reflexiones a respecto del empleo de esta tecnología para fines de vigilancia en el sistema penal. Las contribuciones del estudio indican que los ingenios digitales de vigilancia no se distancian de la lógica punitiva, por el contrario, ellos surgen para componer un diagrama de la punición, configurando una era de la tecnología de control social como política criminal.

Palabras clave*: Biometría de comportamiento; Vigilancia; Criminología crítica.*

1 Introduction

The concept of personality refers to a historical cultural construction marked by the duality between body and soul. Despite the numerous disparate conceptions about this duality, it is a fact that the characterization of the human "being" goes through the biological and psychic complexity of each subject, immersed in a diffuse cultural broth. The body is an organic entity of permanent interaction with the world. The mind formulates ideas, aspires and aspires. Together, mind and body feel, dimension life and mark existence based on choices, gestures and actions that model behaviors that portray personalities. In this context, new technologies point to the possibility of biometrically recognizing the personality of each individual through the parameterization of behavioral externalities. Systems structured on monitoring resources, *big data,* and artificial intelligence suggest that they are capable of this feat.

This technological framework recalls Cesare Lombroso (2013), a nineteenth-century psychiatrist who proposed to recognize delinquency through the bias of body morphological analysis. To a certain extent, the use of new technologies suggests the institution of a new positive school of criminal law, which should be observed with great caution, given that the criminal phenomenon, above all, is established from culturally forged values.

In view of these aspects, this article offers an overview of the trends, benefits and

limitations present in behavioral biometrics proposals and the potential applications in the context of the penal system, whether in relation to criminal activities mediated by information technology, or in the monitoring of people in public and private environments. In this sense, the study considered three specific objectives, which are: a) to explore aspects regarding corporeality as an expressive dimension of individual personality; b) address general technical issues about behavioral biometrics; c) to reflect on the use of this technology for surveillance purposes in the penal system.

The hypothetical-deductive approach method was used in the research (Marconi; Lakatos, 2022), involving elements of contemporary conjunctural reality, in order to evaluate possible solutions to identified problems. The procedures followed the theoretical framework of critical criminology, which questions selective and discriminatory conceptions of the penal system, in the perspective of overcoming the "pathological theories of criminality, [...] based on biological and psychological characteristics that would differentiate 'criminal' subjects from 'normal' individuals" (Baratta, 1997, p. 29). This is an approach that offers important elements on the use of biometric identification technologies, in view of the social principles and values enshrined in the Federal Constitution of 1988.

2 Body, Expression and Personality

Human existence implies being in permanent dialogue with the world. In this sense, understanding reality is something more than a naïve contemplative act, since it is a process of interaction with previous structures (in the hermeneutic sense, pre-comprehensive structure), historically, ideologically and culturally situated, which make the subject part of what he seeks to understand.

For Zea (2001), the human being is defined by history and what he can or cannot be depends on a triple dimension: what gives meaning to the fact, what one does and what one can continue to do. The understanding of history defines choices in the sense of affirming and preserving the past, hope in the present or permanent change in the future. According to Engelmann (2007), the "subject is immersed in history, which justifies his personal tradition and that of the group in which he participates".

From this perspective, the issue of corporeality does not escape. The body is a condition for the possibility of existence. We recognize each one by reason of the characteristics present and manifested by the body. Gestures, ways of acting communicate and, in communicating, constitute identities.

For Laban, the body is "man's first means of communication in his evolutionary process and context", so that "it has a language, which can be articulated in different ways and thus produce different meanings, always gathered under the hegemony of movement"

(Miranda, 2008, p. 17).

> The body expresses itself according to the perceptive movement it performs in the world, because perception is made through a motor attitude, a gesture, from which a practice of habitation and meaning takes place. The body perceives that it is situated in the sensible world, which makes sense to it and, to the extent that it communicates with others, it expresses this perception. What the body communicates, even before words, is the perception of the world. Expression is, then, the gesture with which the body communicates in the world (Reis, p. 137, 2011).

Sometimes we use the word "body" to refer to something that denotes *form* and *structure*, something close to the etymon of the word, which indicates what is apparent. The *corpus* suggests stability and unity, despite the transience that marks existence.

Body is power and, at the same time, limit in a paradoxical cut that crosses human reality. It is important to note that thought (the *Cartesian res cogitans*), linked to verbal language and alphabetic writing, has assumed such strength that the body has been dissociated from the brain and thrown into a subordinate condition in relation to the superior control of the mind (Vidal, 2012).

However, considering what Merleau-Ponty teaches, Furlan and Bocchi (2003, p. 445) state that words do not find meaning in the plane of thought, "it is in the sense of behavior that the meanings of words will always meet, and it is in the agreement of our practical intentions, that is, in the sense of what we do, that communication takes place".

Signification is a social construct that throws the human beyond purely organic processes, culturally materialized "by dances, myths, rituals, commensality, symbolic exchanges, kinship relations, art, religion... It is done for all that, in short, that can only be found within the human universe" (Rodrigues, 1999, p. 97). "Signifying" enters the field of communication from systems of symbols. On the subject, Flusser (2017, p. 126) considers that:

> [...] a code is a system of symbols. Its objective is to enable communication between men. Since symbols are phenomena that replace ("signify") other phenomena, communication is therefore a substitution; it replaces the experience of what it refers to. Men have to understand each other by means of codes, because they have lost direct contact with the meaning of symbols. Man is an "alienated" animal (*verfremdet*) and is forced to create symbols and order them in codes, if he wants to bridge the abyss that exists between him and the "world". He needs to "mediate" (*vermitteln*), he needs to make sense of the "world". Wherever codes are discovered, something can be deduced about humanity.

In this context, "the body means to the world as the world means to the world, the relationship of the being in the world is significant and ambiguous, and the expression derives from this. Expression is the manifest perceptive attitude intersubjectively; it is the expression of being in the world" (Reis, 2012, p. 25). Groh (2019, p. 3) states that "human beings define their identity mainly by the way they present, draw, and stylize their body".

The body in its image, structure and movement is a symbol. The body speaks

(Weil; Tompakow, 1986) based on a motor syntax whose language provides the production of meanings and identities. It is under this assumption that computing, by associating biometric techniques and resources, proposes alternatives for behavioral recognition and prediction.

3 Behavioral Biometrics

To a large extent, human interactions occur through Information and Communication Technologies, breaking barriers of space and time. The benefits obtained from these advances are diametrically proportional to the challenges they reveal in the face of criminal activities. The indiscriminate flow of data and the emergence of the Internet of Things (IoT[1]) raise security concerns for organizations and individuals (Brooks, 2021).

Traditional methods such as access code systems and PIN[2] have proven to be ineffective in the face of advances in techniques and resources for violating computerized systems. On the other hand, the recognition of people from image and video records experiences technological improvements with a view to reducing technical limitations and providing more efficient results. Thus, robust authentication and identification mechanisms based on behavioral biometrics[3] are gaining popularity.

Behavioral biometrics proposes to identify measurable patterns of human activities, companies in choices, gestures, and actions. The term contrasts with strictly physical and static biometrics that involve innate human characteristics such as fingerprint or iris. Behavioral biometric authentication comprises the dynamics of body movements, including singularities in the use of interfaces such as keyboard and mouse, as well as gait analysis among other aspects (Onespan, 2019). By observing the motor and cognitive characteristics of a user, behavioral biometrics are considered one of the safest methods of authentication in the fight against fraud. The technology proposes to distinguish legitimate users and cybercriminals by identifying people based on their online behavior and interaction. In this field, machine learning (*machine learning*[4]) is used to examine patterns of human activity and confirm identity. It also proposes to distinguish the action performed by a human being from

[1] "In general, it can be understood as an environment of physical objects interconnected with the internet through small and embedded sensors, creating an omnipresent (ubiquitous) computing ecosystem, aimed at facilitating people's daily lives, introducing functional solutions in everyday processes. What all IoT definitions have in common is that they focus on how computers, sensors, and objects interact with each other and process information/data in a context of hyperconnectivity" (Magrani, 2018, p. 20).

[2] PIN (*personal identification number*) "is a *string* A relatively short numeric (usually 4 to 8 digits) that is used as a password to authenticate a user on a device such as a smart card, an automated teller machine (ATM), or a mobile phone. Standards that address PIN management and security include ANSI X9.8 and ISO 9564" (Adams, 2011, p. 927).

[3] "The data in a biometric study are usually based on individual observations, which are observations or measurements made at the smallest sampling unit" (Sokal; Rohlf, 2003, p. 8).

[4] It designates "a subset of the use of artificial intelligence, which learns on its own while receiving more data to be able to perform a specific task with increasing precision" (International Business Machines Corporation [IBM], 2022).

that produced by automated resources. Some approaches have stood out such as device-based gestures, vocal patterns, and body kinesthetic patterns.

In device-based gestures, the dynamics of keyboard use can be highlighted, which comprises typing patterns that differ from one person to another. Mixed measurement of speed and time of key actuation and singular typing patterns is performed, as well as cursor movement and speed, usual paths, clicks and interactions. These are examples of patterns that, in a combined way, can identify people (Guilherme, 2016). In turn, vocal patterns are measured from distinct and recurrent sound variations that occur in speech or vocalization.

In the body kinesthetic context, there is the analysis of posture, characteristic of the position of the body and weight distribution of the body in the legs. This can be based on images of poses combined with measurements of the arms and legs, and thermal maps of the joints of the limbs (Tavares, 2021). In this same context, the analysis of the gait recognition is integrated, which corresponds to the recognition of a person's "way of walking" (Controlid, 2020). This includes aspects such as stride length, upper body posture, and walking pace.

The massive use of behavioral biometrics in *e-commerce*, banking systems, and access control organizations is evidenced. Compared to other segments, e-commerce is always on the "bleeding edge[5]" of technology, driven by the purpose of improving the user experience as a competitive differentiating factor.

In the *e-commerce landscape,* there are those who aspire to incorporate behavioral biometrics into the entire customer experience. In the case of banks, the use of behavioral biometrics involves continuous monitoring procedures that confirm the user's identity during an active browsing session on the website and not only at the time of entry.

Febraban states that banking organizations "invest around R$ 25.7 billion annually in technology, of which 10% are focused on cybersecurity" (Nassif, 2022). Financial institutions seek preventive measures to protect account holders from fraudulent access and practices (Cavalcanti, 2022), that is, behavioral biometrics allow the entire user journey to be evaluated in real time, from the moment of access to the platform (start of a session), to the completion of a transaction (Proviti, 2021).

Regarding *gait recognition* systems, behavioral biometrics can be used as an effective means of access control. By studying walking patterns, access can be granted quickly, reducing bottlenecks in congested common areas. In addition to presenting advantages over other biometrics, such as facial recognition, fingerprint or iris, the recognition of people by the way they walk makes it possible to obtain biometric characteristics at a distance in a non-invasive way,

[5] In the technological field, "*bleeding edge*" is the expression used to designate "cutting-edge" technology. Kenton (2021) observes that it is "[...] a type of technology released to the public, although it has not been thoroughly tested and may not be reliable. Cutting-edge technology often comes with a degree of risk and expense for the end user – in most cases, the consumer."

without the need for high-resolution images (Nunes, 2011).

4 Behavioral Biometrics, Surveillance, and Crime

The rationality that guides criminal law must consider, among other aspects, freedom and existential dignity as its structuring assumptions. This results, among other aspects, in the presumption of innocence in the face of evidentiary doubt and the application of the most lenient penalty on facts subject to multiple typifications. The rule of law has in the protection of individual freedom one of its greatest assets, subject to restrictive parameters only exceptionally for its own safeguard.

Therefore, the power of the State, or of those who act on its behalf, does not materialize indiscriminately. It can be said that there is no "will" of the State, in the Kantian sense of the term (Kant, 2002) that can demand a conduct or punish, whose foundation is not the democratic expression, embodied in the law. Under this primacy, it has long been considered that "it is for each one the right to be subject only to the laws, to be neither arrested, nor detained, nor killed, nor ill-treated in any way, due to the arbitrary will of one or several individuals" (Constant, 2015, p. 77).

The exercise of all freedom is part of the commitment of each one to participate in the preservation of the freedom of the other, so that no person is immune to the consequences of his actions, in the same perspective that anonymity is not admitted for the free exercise of the expression of thought (art. 5, IV, CF/1988).

From this perspective, the recognition of authorship over action is a social commitment. No one can act anonymously against the dignity of the other and against the legal order itself, under the pretext of self-determination or the guarantee of privacy.

The State has a monopoly on the use of force, as well as the exercise of police power, which includes the use of means and resources that, in favor of the public interest, necessarily mitigate the exercise of individual freedoms. However, the question that arises is to recognize to what extent the police activity preserves its legitimacy, without compromising the fundamental assumption of guaranteeing individual freedoms.

It is under this reality that the debate about the application of surveillance technologies is inserted. Technological resources make social exchange based on permanent monitoring even more sophisticated as a necessary condition for guaranteeing benefits and security. In this context, Rodotà (2008, p. 24) observes that "the very organizational fabric of power, resinified by the information infrastructure itself as a fundamental component" comes into play.

Lyon (2014, p. 6) observes that:

> Surveillance is a key dimension of the modern world; Travelers passing through airports everywhere know they have to wade through not only passport control in its 21st-century version, but also through new devices, such as body scanners and biometric screening devices, that have proliferated since Sept. 11. And if all this has to do with security, other types of surveillance, related to routine and common purchases, online access or participation in social media, are also becoming increasingly ubiquitous. We have to show identity documents, enter passwords, and use coded controls in numerous contexts, from shopping online to entering buildings. Every day Google annotates our searches, stimulating customized marketing strategies.

Just as surveillance in the spaces of large workshops and factories has become a defined function, inherent to the sophistication of production processes, as Foucault (1987) argues, it also becomes part of the complexity of consumer relations and technologically instrumentalized life itself. For Foucault (1987), all surveillance spaces help in the control of bodies and in the identification of those who want to be punished, and all this feeds a penal system made up of the police, ministerial, judicial and prison apparatuses.

This penal system that everyone is subject to, generates bodies identified and stigmatized by location techniques (surveillance cameras in public and private spaces), biometric identification techniques and body scanners. Andrade (1999) points out that this system promises an illusion of public security against crime, claiming that it protects general legal assets and fights crime (the "evil") in defense of society (the "good") through general prevention (intimidation of potential offenders) and special prevention (rehabilitation of convicts), because: “It appears, simultaneously, as a system operationalized within the limits of legality, legal equality and other liberal principles that guarantee and, therefore, as a promise of legal certainty for those criminalized” (Andrade, 1999, p. 30-31).

Added to these factors is the persistence of a punitive culture whose transformation has received contributions from critical criminological thinking that, since the sixties, has sought to overcome the etiological model, elaborating knowledge committed to transformations in the social, cultural and ideological basis of the formation and application of criminal law.

From critical criminology, it is possible to unveil the operationality and real functions of the penal system, this dynamic of the ideological functioning of the system that is there, which operates when it socially justifies its importance and hides its real and inverted functions, which Andrade calls the "illusion of security", which creates a Manichean division between the (sub) world of criminality, identified with a minority of potentially dangerous subjects (evil) and the world of normality, represented by the majority of society (good), discourse of an "ideology of control" (Andrade, 1999, p. 30).

This control of conduct through technologies, associated with a culture of punishment, is the favorable terrain for the most varied atrocities, and even forms of manifestation of racism, such as the fact investigated by the Civil Police of Ceará in the Zara

stores of Shopping Iguatemi Fortaleza. It is the creation of an alert code so that employees could be secretly informed about the entry of black people or people with "simple clothes" into the establishment. The secret code, "Zara Zerou", was advertised on the store's sound system (Folhapress, 2021). In the same sense, Baratta (1997) argues that the selection process criminalizes (primarily and secondarily) vulnerable sectors, allowing the broad immunization of those sectors resistant to the system. This vulnerability is inversely proportional to the holding of political and/or economic and/or scientific power. These immune sectors, which nevertheless practice behaviors considered socially negative, will be part of the so-called hidden criminality. This is the logic of the system, as it would be impossible to pursue and sentence all actions and omissions, since, as Zaffaroni (1991) rightly observes, the organs of the penal system "exercise their militarizing and verticalizing-disciplinary power and this means that their power to configure generally falls on the poorest sectors of the population and on some dissidents (or different) who are more uncomfortable or significant" (Zaffaroni, 1991, p. 23-24).

Another concern is about errors that have already occurred in the identification of people, when the penal system needs to operate within the constitutional parameters of strict legality and the dignity of the human person. Crime is inherent to all societies, and the choice of crimes that the State will punish is of a political-legislative order.

In view of this, there is the selectivity of those criminalized through the arms of the system's control agencies supported by identification technologies.

However, authentication and monitoring systems have massively integrated daily life with the purpose of providing benefits to consumers in electronic media. In this context, security becomes directly and indirectly a product. It so happens that, provided by Information Technologies, security presupposes the appropriation and control of information that concerns the users of these same technologies.

Enabling social interaction through the informational technological apparatus means more than offering tools for communication, it is providing means that transfigure one's own being. Lanier (2012, p. 20) states that computer technologists, programmers and designers create "extensions to being", which consist of the structures from which people begin to perceive the world and themselves. Thus, digital coexistence is increasingly presented as reality and not virtuality. A *priori*, the virtual corresponds to a "representative" dimension of a given reality. In this sense, everything that does not fully integrate the most significant attributes of what is real is considered virtual. The virtual, as well as the images, corresponds to a representation of the real (Wolff, 2004). However, some human activities come to exist primarily (or only) in digital media, which gives this plane no longer the *status* of virtuality, but of reality.

It turns out that this digital reality is highly subject to manipulation by those who know the languages, codes, and protocols that sustain it. Considering these factors, there is no denying that the improvement of Digital Surveillance and Monitoring Technologies, paradoxically, tends to

offer technical conditions that are themselves subject to deviations in application. In other words, the more technologies are developed to provide security, the more technical conditions are instituted in order to enable weaknesses, since security by digital means presupposes the mastery and control of reality itself.

The appeal to behavioral biometrics is guided by the benefits of the strict technique, which provides greater efficiency under the domain of recognizing individuals through machines. Ensuring that this instrumental domain is employed only for legitimate purposes is not something that technology can endorse.

To deal with this dilemma, one of the principles mentioned in international debates on the development and use of artificial intelligence (UNESCO, 2022), as well as in the context of the elaboration of the regulatory framework for artificial intelligence in Brazil (Agência Senado, 2022), can also be considered here. It is the principle of transparency in the face of the assumptions and mechanisms from which the processing of data on digital platforms operates. Although the current Data Protection Law (Brazil, Law No. 13,709/2018) already establishes parameters in this regard, it does so especially in relation to data, without determining the publicity of processing processes and mechanisms.

Another path is to define restrictive parameters on the use of technologies for biometric identification. Thus, in the context of the negotiations for the regulation of artificial intelligence in Europe, the issue is based on three levels of risk on AI: *unacceptable risk, high risk, and limited risk*. In this context, the use of AI for biometric identification is recognized as an "unacceptable risk" and, therefore, should not be admitted[6], either for the categorization of people or for biometric identification in public spaces, remotely and in real time. For "post" remote biometric identification, which consists of recognizing the person at a time/place other than the registration of the biometric data, the identification will be admitted for the purposes of criminal prosecution, provided that it involves serious crimes and the identification is previously authorized by the courts (European Parliament, 2023).

Thus, it is verified that the issue is complex because it assumes consequences on how social subjects are informed and can objectively have guaranteed the reservation of data that concerns their personalities, in the face of digital procedures of capture, treatment and storage, for persecutory purposes of behavioral biometric identification.

[6] The use of technology is permitted for the following cases: "(i) targeted search of potential victims of crime, including missing children, (ii) to prevent a specific, substantial and imminent threat to the life or physical safety of persons or of a terrorist attack, and (iii) for the detection, location, identification or prosecution of a perpetrator or individual suspected of a crime" (European Parliament, 2023).

5 Final Thoughts

The State's action to reduce crime goes through several perspectives and approaches, among which are preventive and repressive actions. Thus, the use of Recognition technologies, especially those based on behavioral biometrics, may not meet, *a priori*, the expectations of improvement of the penal system, at least with regard to the reduction of crime. Although its potential in terms of efficiency in the recognition of people is technically attested, including a suggestive potential for criminal probability, the social price of this instrumentalization can be very high.

As a rule, behavioral biometrics presupposes the institution of a dynamic information base linked to a permanent monitoring system, capable of constant production and updating of behavioral patterns, via *machine learning*. Despite being referred to as one of the safest methods of combating fraud, the fact is that such a system both presupposes and tends to feed back a positivist approach to criminal law, whose ideological maxim is based on the fetish of the delinquent subject and the criminal profile.

It is evident that we live in the era of social control technology, with techniques for managing the amount of data (*big data*), nanotechnology (*microchips*), among others. However, it is important to emphasize that these technologies are used both by the agencies of the penal system, but also by criminal activity, which has appropriated technology to commit harmful and even lethal actions, which is causing great alarm oriented towards the demand for greater social control.

It cannot be denied the existence of criminal conduct and recurrence and that criminality in the digital environment demands advanced technological resources. However, deep social inequalities of an economic, ethnic, and cultural nature mark the Brazilian reality and are intertwined with the picture of criminality, so that the parameters, requirements, and conditions for the application of surveillance technologies based on behavioral biometrics deserve a restrictive approach.

The technological increase of any of them points to the necessary consideration of the impacts that technologies can generate, not only in terms of immediate operational efficiency, but also on the implications and reflex weaknesses, and more especially in terms of the effectiveness of the social principles and values enshrined in the Federal Constitution of 1988.

References

ADAMS, Carlisle. Personal Identification Number (PIN). *In*: VAN TILBORG, Henk C. A.;

JAJODIA, Sushil (eds.) **Encyclopedia of cryptography and security**. Boston: Springer, 2011. p. 458. DOI: https://doi. org/10.1007/978-1-4419-5906-5_91. Accessed on: May 16, 2022.

ANDRADE, Vera Regina Pereira de. The social construction of agrarian conflicts as criminality. *In*: SANTOS, Rogério Dutra dos (ed.). **Critical introduction to the study of the penal system**: elements for understanding the repressive activity of the State. Florianópolis: Legal Diploma, 1999. p. 23-54.

ANTI-FRAUD behavioral biometrics. **Protiviti**, [*s. l.*], 2021. Available at: https://www.protiviti.com/ BR-por/performance-empresarial/protecao-ao-e-commerce/biometria-comportamental-antifraude. Accessed on: May 16, 2022.

BARATTA, Alessandro. **Critical criminology and criticism of criminal law**: introduction to the sociology of criminal law. Translation: Juarez Cirino dos Santos. Rio de Janeiro: Revan, 1997.

BEHAVIORAL biometrics: frictionless security in the fight against fraud. **OneSpan**, [*s. l.*], 2019. Available at: https://www.onespan.com/pt-br/resources/biometria-comportamental-seguranca-sem-atrito-no-combate-fraudes. Accessed on: May 16, 2022.

BRAZIL. [Constitution (1988)]. **Constitution of the Federative Republic of Brazil of 1988**. Brasília, DF: President of the Republic, [2016]. Available at: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao. htm. Accessed on 22 May 2022.

BRAZIL. **Law No. 13,709, of August 14, 2018**. General Law for the Protection of Personal Data (LGPD). Brasília, DF: Presidency of the Republic, [2022]. Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Accessed on: 22 May 2022.

BROOKS, Chuck. MORE Alarming Cybersecurity Stats For 2021! **Forbes**, [*s. l.*], 24 Oct. 2021. Available at: https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-. Accessed on: May 16, 2022.

CAVALCANTI, Cassiano. Behavioral biometrics help banks identify potential situations of customers' danger. **Crypto ID**, [*s. l.*], 7 mar. 2022. Available at: https://cryptoid.com.br/biometria-2/ behavioral-biometrics-helps-banks-to-identify-possible-danger-situations-of-customers/. Accessed on: May 16, 2022.

CONSTANT, Benjamin. **The freedom of the ancients compared to that of the moderns**. Translation: Emerson Garcia. São Paulo: Atlas, 2015.

ENGELMANN, Wilson. **Natural law, ethics and hermeneutics**. Porto Alegre: Livraria do Advogado, 2007.

CONTROLID TEAM. Get to know the recognition system by the "way you walk". **Control iD**, [s. l.], 22 May 2020. Available at: https://www.controlid.com.br/blog/biometria/ recognition-way-of-walking/. Accessed on: May 17, 2022.

EUROPEAN PARLIAMENT. EU AI Act: First regulation of artificial intelligence. **News European Parliament**, [*s.l.*], 18 Dec. 2023. Available at: https://www.europarl.europa.eu/news/pt/headlines/ society/20230601STO93804/lei-da-eu-sobre-ia-primeira-regulacao-de-inteligencia-artificial. Access on: 18 Jan. 2024.

FLUSSER, Vilém. **The Codified World**: For a Philosophy of Design and Communication. Translation: Raquel Abi-Sâmara. São Paulo: Ubu Editora, 2017.

FOLHAPRESS. Zara is investigated after creating a secret code to alert blacks to enter the store. **NSC Total**, [*s. l.*], 21 nov. 2021. Available at: https://www.nsctotal.com.br/noticias/zara-e-investigada-apos-criar-codigo-secreto-para-alertar-entrada-de-negros-em-loja . Accessed on: 23 May 2022.

FOUCAULT, Michel. **To watch and punish:** the birth of prison. Translation: Raquel Ramalhete. Petrópolis: Vozes, 1987.

FURLAN, Reinaldo; BOCCHI, Josiane Cristina. The body as expression and language in Merleau-Ponty. **Estudos de Psicologia**, Natal, v. 8, n. 3, p. 445-450, 2003. DOI: https://doi.org/10.1590/S1413-294X2003000300011. Available at: https://www.scielo.br/j/epsic/a/RmBNRmVhDydstrCX9wB6j3B/?lang=pt. Accessed on: 8 May 2022.

GROH, Arnold. Cultural identity and the body. **Revista Psicologia e Saúde**, [*s. l.*], v. 11, n. 2, p. 3-22, 17 jul. 2019. DOI: https://doi.org/10.20435/pssa.v11i2.907. Available at: https://pssaucdb.emnuvens.com.br/pssa/ article/view/907. Accessed on: May 16, 2022.

GUILHERME, Paulo. The movement of your mouse can reveal who you are in Tor. **Tec Mundo**, [*s. l.*], 11 mar. 2016. Available at: https://www.tecmundo.com.br/seguranca-de-dados/102216-movimento-mouse-revelar-voce-tor.htm . Accessed on: May 16, 2022.

KANT, Immanuel. **Critique of practical reason**. Translation: Valério Rohden. São Paulo: Martins Fontes, 2002.

KENTON, Will. Bleeding edge technology: meaning, cost, benefits. **Investopedia**, [*s. l.*], 8 Apr. 2021. Available at: https://www.investopedia.com/terms/b/bleeding-edge-technology.asp Accessed on: 20 May. 2022.

LANIER, Jaron. **Welcome to the Future**: A Humanistic View on the Advancement of Technology. Translation: Cristina Yamagami. São Paulo: Saraiva, 2012.

LOMBROSO, Cesare. **The delinquent man**. Translation: Sebastião José Roque. São Paulo: Icon, 2013.

LYON, David. Introduction. *In*: BAUMAN, Zygmunt; LUON, David. **Liquid surveillance**: dialogues with David Lyon. Translation: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014. p. 9-16.

MAGRANI, Eduardo. **The internet of things**. Rio de Janeiro: FGV Editora, 2018. *E-book*. Available at: https:// bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A internet of coisas.pdf. Accessed on: 10 Apr. 2022.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Scientific methodology**. 8. ed. Barueri: Atlas, 2022. MIRANDA, Regina. **Body-space**: aspects of a geophilosophy of motion. Rio de Janeiro: 7Letras, 2008.

NASSIF, Tamara. Digital scams put cybersecurity to the test. **CNN Brasil**, São Paulo, 19 Apr. 2022. Available at: https://www.cnnbrasil.com.br/business/golpes-digitais-colocam-ciberseguranca-a-prova-veja-how-to-protect/ Accessed on: 19 May 2022.

NUNES, Rodrigo Alves. **Evaluation of techniques for the recognition of people by the**

way they walk (*Gait Recognition*). 2011. Dissertation (Master's Degree in Informatics) - Graduate Program in Informatics, Federal University of Paraná, Curitiba, 2011. Available at: http://hdl.handle.net/1884/25832. Accessed on: May 16, 2022.

REIS, Nayara Borges. **Expression and being in the world in the phenomenology of perception**. 2012. Dissertation (Master's Degree in Philosophy) - Institute of Philosophy and Human Sciences, Federal University of Bahia, Salvador, 2012. Available at: https://ppgf.ufba.br/sites/ppgfilosofia.ufba.br/files/nayara_borges.pdf. Accessed on: May 16, 2022.

REIS, Nayara Borges. The body as expression according to Merleau-Ponty's philosophy. **Kínesis**, Marília, v. III, n. 6, p. 137-153, dez. 2011. DOI: https://doi.org/10.36311/1984-8900.2011.v3n06.4429. Available at: https:// revistas.marilia.unesp.br/index.php/kinesis/article/view/4429. Accessed on: June 10, 2022.

RODOTÀ, Stefano. **Life in the surveillance society**: privacy today. Rio de Janeiro: Renovar, 2008.

RODRIGUES, José Carlos. **The body in history.** Rio de Janeiro: Editora FIOCRUZ, 1999. DOI: https://doi. org/10.7476/9788575415559. Available at: https://books.scielo.org/id/p9949. Accessed on: 8 May 2022.

SENATE AGENCY. Brazil may have a regulatory framework for artificial intelligence. **Senado Notícias**, Brasília, 30 mar. 2022. Available at: https://www12.senado.leg.br/noticias/materias/2022/03/30/brasil-podera-ter-marco-regulio-para-inteligencia-artificial . Accessed on: 22 May 2022.

SOKAL, Robert R.; ROHLF, F. James. **Biometry**: the principles and practice of statistics in biological research. 3rd ed. New York: W. H. Freeman and Company, 2003.

TAVARES, Henrique Leal. **Identification of people based on anthropometric and gait features extracted from 2D poses**. 2021. Dissertation (Master's Degree in Computer Science) - Graduate Program in Computer Science, São Paulo State University "Júlio de Mesquita Filho", Bauru. 2021. Available at: http://hdl.handle.net/11449/214430 Accessed on: May 17, 2022.

TYPES of artificial intelligence and applications. **IBM,** [*s. l.*], 2022. Available at: https://www.ibm.com/br-pt/ analytics/journey-to-ai. Accessed on: 8 Feb. 2022.

UNESCO. **Recommendation on the Ethics of Artificial Intelligence**. Paris: UNESCO, 2022. Available at: https://es.unesco.org/artificial-intelligence/ethics. Accessed on: May 16, 2022.

VIDAL, Fernando. The cerebral subject: a historical and conceptual sketch. **Polis and Psyche**, Porto Alegre, v. 1, n. 1, p. 169-190, 2011. DOI: https://doi.org/10.22456/2238-152X.25883. Available at: https://seer.ufrgs.br/ PolisePsique/article/view/25883. Accessed on: May 16, 2022.

WEIL, Pierre; TOMPAKOW, Roland. **The body speaks**: the silent language of nonverbal communication. Petrópolis: Vozes, 1986.

WOLFF, Francis. Behind the show: the power of images. *In*: NOVAES, Adauto (ed.). **Far beyond the spectacle**. São Paulo: Editora Senac, 2004. p. 17-45.

ZAFFARONI, Eugenio Raul. **In search of lost sentences:** the loss of legitimacy of the penal

system. Translation: Vânia Romano Pedrosa and Amir Lopes da Conceição. Rio de Janeiro: Revan, 1991.

ZEA, Leopoldo. **Discourse from marginalization and barbarism**. São Paulo: Garamond, 2001.

How to cite:

ARRABAL, Alejandro Knaesel; KELNER, Lenice; SILVA, Leandro Felix da. Crime, Surveillance and Technologies of Behavioral Biometric Recognition. **Pensar – Journal of Legal Sciences**, Fortaleza, v. 29, n. 1, p. 1-11, jan./mar. 2024. DOI: https://doi.org/10.5020/2317-2150.2024.16823

Mailing address:

Alejandro Knaesel Arrabal - Email: arrabal@furb.br

Lenice Kelner - Email: kelner@furb.br

Leandro Felix da Silva - Email: contato@leandrofelix.com.br

Received: *09/03/2023*
Accepted on: *01/05/2024*