NEW BODY PERIMETER AND BIOMETRICS AS PERSONAL DATA: SOME THOUGHTS AND INSIGHTS ON THE 'SÃO PAULO METRO CASE'

Cristiano Colombo [*]
Guilherme Damasio Goulart [**]

Abstract: This article deals with the new body perimeter and biometrics as personal data, seeking, from a principled point of view, to present recommendations for the application of facial recognition in the São Paulo Metro. Balancing the impacts of biometric techniques and the principles of purpose and necessity of the Brazilian General Data Protection Law, the following question arises: can facial biometrics be applied on the premises of the São Paulo Metro? And, if the answer is positive, what would be its limits, based on the aforementioned principles? With regard to methodology, the research was theoretical, dealing with the theme in an exploratory and descriptive way, making use of bibliographic technical procedures.

Keywords: biometrics; data protection; São Paulo metro case.

INTRODUCTION

This article deals with the new body perimeter and biometrics as personal data, and aims to present recommendations for the use of facial recognition in the São Paulo Metro, based on a principiological perspective. In light of the balance between biometric techniques and the principles of purpose and necessity outlined in Article 6 of the Brazilian General Data Protection Law, the following question arises: can facial biometrics be used in the São Paulo Metro? And, if the answer is yes, what would be its limits based on the principiological basis of the LGPD, particularly the principles of purpose and necessity?

In the first part, the new body perimeter will be analyzed from physical and electronic perspectives, viewing it as a dual and indivisible whole linked to a person, as well as biometrics as personal data, especially because it uses "a unique individual characteristic for identification and/or authentication"

[*] Ph.D, Federal University of Rio Grande do Sul (UFRGS); Professor, University of Vale do Rio dos Sinos (UNISINOS). Email: cristianocolombo@unisinos.br / ORCID iD: https://orcid.org/0000-0002-4362-0459

[**] Ph.D, Federal University of Rio Grande do Sul (UFRGS); Lawyer, professor, and consultant in Information Security, Technology Law, and Personal Data Protection. Email: guilherme@direitodatecnologia.com / ORCID iD: https://orcid.org/0000-0001-6724-9335

which can be erased from consultation databases, however, sources "generally cannot be changed or suppressed." In the second part, recommendations will be made about the use of biometrics in the São Paulo Metro, based on the interpretive foundation of the principles of purpose and necessity.

The research method was theoretical, exploring and describing the topic using bibliographical techniques.

I. BODY, TECHNOLOGY, AND PERSONAL DATA

A. New Body Perimeter

Despite the person being a complex[1] unit that requires comprehensive protection[2], the body, as a physical support[3] that embodies[4] the person, has specific protection in the scope of personality rights. At the very beginning of the Brazilian Civil Code[5], in articles 13 to 15, aspects of body protection are dealt with, initially prohibiting what are called acts of disposition "when they result in permanent physical degradation or go against good customs." As is also known, throughout history, the legal treatment of the body has undergone several changes until it has reached, in the present day, to "bodily integrity in the field of subject autonomy."[6]

The body can also be seen as a means of expressing personality and personal identity[7]. When speaking of private autonomy, there is a power

[1] Souza, Rabindranath V.A. Capelo de. O Direito Geral de Personalidade. Coimbra: Coimbra, 2011, 211.

[2] Through the "protection of psychophysical integrity", cf. Perlingieri, Pietro. O Direito Civil na legalidade constitucional. Translated by Maria Cristina de Cicco. Rio de Janeiro: Renovar, 2008, 776.

[3] The organic part that constitutes its physical support, cf. Cifuentes, Santos. Elementos de derecho civil: Parte general. 4th ed. Buenos Aires: Astrea, 1999, 64.

[4] As the body, therefore, is "legally protected", cf. Perlingieri, Pietro. O Direito Civil na legalidade constitucional. Translated by Maria Cristina de Cicco. Rio de Janeiro: Renovar, 2008, 776.

[5] Remembering that the protection of the body is also a concern of Criminal Law in several different laws.

[6] Schreiber, Anderson, et al. Código Civil Comentado: Doutrina e Jurisprudência. 3rd ed. Rio de Janeiro: Forense, 2021. The author cites examples, mainly related to "psychophysical integrity" that are present in several different legislations and legal commands. See also the Brazilian classic on the subject, Chaves, Antônio. Direito à vida e ao próprio corpo (Intersexualidade, transexualidade, transplantes). 2nd ed. São Paulo: Revista dos Tribunais, 1994.

[7] The concept of personal identity was initially derived from the name, being one of the most important expressions of its development Adriano de Cupis, including a specific work on the subject, namely De Cupis, Adriano. Il Diritto all'Identità Personale. Milan: Dott. A. Giuffrè, 1949. A more contemporary meaning of this right can be seen, among others, in

conferred upon the person to, within the limits of human dignity, make choices that may involve the body itself[8], within the limits of the legal order[9]. It is noted that this autonomy also comprises what is called "free development of personality," recognized, at least among Portuguese speakers, as a fundamental right[10] and in Brazil as an implicit principle in the Federal Constitution[11], specifically provided in Article 1 of the LGPD[12]. This is a right, according to Mota Pinto, that involves the freest expression of humanity, "something that institutes or builds itself, according to its own project, determined from the person itself as an autonomous decision-making center."[13] Autonomy is identified in this context when related to existing legal situations or relationships, such as the so-called "self-determination."[14] This self-determination, in general, is already recognized by the best doctrine in relation to the body itself[15]. Therefore, consent in relation to the physical

---

Almeida, José Luiz Gavião de, Luis Renato Vedovato, and Marcelo Rodrigues da Silva. "A identidade pessoal como direito fundamental da pessoa humana e algumas de suas manifestações na ordem jurídica brasileira." Revista de Direito Civil Contemporâneo, vol. 14, 33-70, January-March 2018, 2: "(…) identidade pessoal é "o conjunto fidedigno, adequado e necessário de atributos/"sinais identificadores", eventos e experiências vividas relacionados a determinada pessoa, que tem por escopo realizar de forma estável a sua projeção dignamente perante a sociedade e o Estado, distinguindo-a das outras pessoas e permitindo-lhe, por meio de seu reconhecimento e autorreconhecimento, a sua integração, interação e percepção no meio social e estatal".

[8] Sarmento, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e metodologia. 3rd ed. Belo Horizonte: Fórum, 2016, 142.

[9] Italian doctrine recognizes that human dignity applied to the physical body also applies to the electronic body, cf. Marini, Giovanni. "Commento di Artt. 3-186." In Commentario del Codice Civile. Delle Persone, edited by Angelo Barb and Stefano Pagliantini, Torino: UTET, 2013, 203: "L'inviolabilità della dignità della persona si realizza così nell'inviolabilità del corpo. La dignità esalta il controllo del "corpo elettronico", cioè l'insieme delle informazioni che costruiscono la propria identità. L'identità infatti non deve essere sottomessa a poteri esterni che possono alterarla, falsificarla […]".

[10] Mota Pinto, Paulo. "O Direito ao Livre Desenvolvimento da Personalidade." In Boletim da Faculdade de Direito de Coimbra, Portugal-Brasil Ano 2000, 149-246, 1999, 150.

[11] Cf. Ludwig, Marcos de Campos. "O Direito ao Livre Desenvolvimento da Personalidade na Alemanha e Possibilidades de sua Aplicação no Direito Privado Brasileiro." Revista da Faculdade de Direito da UFRGS, vol. 19, 237-63, March 2001.

[12] Remembering that in the Brazilian Internet Civil Framework (Law no. 12,965/2014), art. 2nd, inc. II, "personality development" is envisaged as one of the fundamentals of Internet use in Brazil.

[13] Mota Pinto, Paulo. "O Direito ao Livre Desenvolvimento da Personalidade."..., 152.

[14] Cf. Bucar, Daniel and Teixeira, Daniele Chaves. "Autonomia e Solidariedade." In O direito Civil - Entre o Sujeito e a Pessoa: Estudos em homenagem ao professor Stefano Rodotà, edited by Gustavo Tepedino, Ana Carolina Brochado de, and Vitor Almeida. Belo Horizonte: Fórum, 2016, 107.

[15] Souza, Rabindranath V.A. Capelo de. O Direito Geral de Personalidade..., 218. The author also indicates that in addition to self-determination, in relation to the body, the person has the right to defend their "corporal integrity or safety". This self-determination can reach,

body is an extremely important requirement to be verified in various contexts, since its absence can be precisely the difference between a lawful act and an unlawful act[16], always remembering that the legal order does not grant an unlimited power of self-determination.[17] In general, the doctrine also recognizes that man is a being in realization and that such realization would attract to itself a teleological vocation.[18]

However, with the evolution of society and computerization, there has been, in Rodotà's words, a transfer of the body and, to some extent, its identity to digital media[19]. The idea of personality rights seen as corporal and incorporeal[20] breaks down with the evolution towards a symbiosis between the two (which could apply to personal data in general). The physical and electronic perspectives vibrate and interweave, building a dual and indivisible whole, linked to a personality. The traditional idea of a "physical unity" or a "skin-defined perimeter" is no longer sufficient for defining and delimiting the body.[21] The electronic body becomes recognized as the "set of information that builds our identity."[22] It is not a "digital twin," but rather an

in some cases, even vital interferences, such as those related to sexual reassignment. On the topic see Choeri, Raul Cleber da Silva. O conceito de identidade e a redesignação sexual. Rio de Janeiro: Renovar, 2004, 23. In his reflections, this author states that "identity becomes a mobile celebration, defined historically rather than biologically. This causes the individual to assume, at different times, different entities, whose characteristic is not to be unified around a coherent self".

[16] Souza, Rabindranath V.A. Capelo de. O Direito Geral de Personalidade..., 218: "Também deve ser algo de especial cuidado a relevância do consentimento do lesado na lesão, e, em certos casos, da sua vontade presumível, como causas de exclusão do facto ilícito ou como causas justificativas da ilicitude".

[17] Souza, Rabindranath V.A. Capelo de. O Direito Geral de Personalidade..., 225.

[18] Gonçalves, Diogo Costa. Pessoa e Direitos de Personalidade: Fundamentação Ontológica da Tutela. Coimbra: Almedina, 2008, 50-51: "Uma das experiências mais marcantes e constantes da realidade humana é a realização da própria vida".

[19] Rodotà, Stefano. "Transformações do Corpo." Revista Trimestral de Direito Civil, Rio de Janeiro 19 (July-September 2004): 91-107.

[20] Cf. Chaves, Antônio. Direito à vida e ao próprio corpo (Intersexualidade, transexualidade, transplantes). 2nd ed. São Paulo: Revista dos Tribunais, 1994.

[21] Rodotà, Stefano. Il diritto di avere diritti. Rome: Laterza, 2012, 26: "L'unità fisica, il perimetro delineato dalla pelle, non definiscono più lo spazio del corpo, che si dilata in un altrove che esige un continuo e paziente lavoro di riconoscimento: chi governa le parti del corpo collocate in quell'«altrove» costituito dalle banche del sangue, del cordone ombelicale, dei gameti, degli embrioni, delle cellule, dei tessuti? Diremo che il corpo occupa il mondo?"

[22] Rodotà, Stefano. Vivere la democrazia. Rome: Laterza & Figli, 2018, digital edition, pos. 207. The author goes on to indicate, when citing the Charter of Fundamental Rights of the European Union, that it "ha ribadito il divieto di fare del corpo un oggetto di profitto. Previsto per il corpo fisico, questo principio può essere esteso al corpo elettronico, come già fanno alcune norme, come quelle che prevedono un'autorizzazione pubblica per trattare i cosiddetti dati sensibili, che riguardano gli aspetti più intimi della vita o la collocazione sociale della persona. Qui il principio di dignità si congiunge con quello di eguaglianza, per

"instant representation of a lifetime's journey."[23] If the idea of an electronic body is already known and well established in Rodotà's doctrine, its expansion to biometric data is almost automatic. This also makes it possible to think of a digital identity[24], which is derived from this construction possible by personal data that is treated in various possible ways. The exercises of personality development and identity construction (digital?) can be expanded in digital media, given the possibilities given to the subject.[25] It is possible to think about the possibility of a person who likes a type of subject to build their social networks based on that theme. The person can even experiment with greater ease and freedom new personas in virtual environments[26], expressing even desires that they would not do in traditional media. In addition, companies that monetize personal data in their business seek to increasingly understand these aspects of their users' "electronic bodies."

This expression of identity was recognized by the Italian *Dichiarazione dei diritti in Internet*, which establishes the "right to identity," stating that "every person has the right to an integral and updated representation of their own identities on the network."[27] It should be noted that the text uses "identities" and not just "identity," which implies this multiple aspect of "identities," of experiments and of the contexts and systems in which these identities are inserted.

The person also exercises control over their digital body through their private autonomy, just as they do with their physical body. However, the beams of protection are obviously different. People have a greater freedom to shape and modify their "electronic body"[28] compared to their physical-

---

evitare discriminazioni o stigmatizzazioni sociali.".

[23] Rodotà, Stefano. Il mondo nella rete. Quali i diritti, quali i vincoli. Rome: Laterza & Figli, 2014, 46.

[24] Rodotà, Stefano. Il mondo nella rete..., 197": "Il «corpo elettronico», l'insieme delle informazioni che costruiscono la nostra identità".

[25] Breton, David. La sociologie du corps. 8th ed. Paris: PUF, 2012. Digital edition, pos. 169.6: "Pour la mouvance transhumaniste notamment, la condition humaine est une cristallisation d'informations pures. Dès lors, ses adeptes visent l'immortalité de l'esprit en considérant que les informations contenues dans le cerveau seront un jour transportables sur un support informatique".

[26] Floridi, Luciano. "The Construction of Personal Identities Online." Minds & Machines, vol. 21, no. 1, 477-79, 2011, 477.

[27] Italy. Camera dei Deputati. "Dichiarazione dei diritti in Internet." Available at https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf. Access on: March 29, 2022.

[28] Breton, David. La sociologie du corps..., pos. 166.9.: "Le corps est surnuméraire pour certains courants de la cyberculture appelant de leurs vœux l'émergence prochaine d'une humanité (que certains appellent déjà une posthumanité) enfin parvenue à se défaire de toutes ses entraves dont la plus cuisante serait le fardeau d'un corps désormais anachronique, fossile".

biological body. Of course, this does not detract from the fact that the subject, according to Rodotà, has "the strong right to never lose the power to maintain full control over their body that is, at the same time, 'physical' and 'electronic.'"[29]

Anyway, digital means expand the possibilities of shaping and manifestation of personal identity greatly.[30] The connection of the idea of the electronic body with the possibilities of creating digital avatars and personas has already been observed.[31] The investigation of biometric data as personal data is now underway.

A. Biometrics as Personal Data

The growth in the use of biometric techniques has mainly occurred due to them becoming more economically accessible, especially due to the increase in data storage and processing capacities, as well as the low cost of fingerprint readers and electronic devices in general.[32] From the analysis of the General Data Protection Law (LGPD), it can be seen that the "biometric" data appears only once, in Article 5, II, when classified as sensitive data, however, without any definition. Based on Opinion 4/2007 on personal data, biometric data is defined as:

> Biological properties, physiological characteristics, physical features or reproducible actions, to the extent that these characteristics and/or actions are simultaneously unique to that person and measurable, even if the patterns used in practice to measure them technically involve a certain degree of probability.[33]

As can be seen, the peculiar feature of biometrics is that the personal data collected "by its very nature, are directly related to each particular person"[34]

---

[29] Rodotà, Stefano. "Transformações do Corpo"…, 97.

[30] Personal identity is regarded as "conjunto de atributos y características que permiten individualizar a la persona en sociedad. Identidad personal es todo aquello que hace que cada cual sea 'uno mismo' y no 'otro". Este plexo de características de la personalidad de 'cada cual" se proyecta hacia el mundo exterior, se fenomenzaliza [...]", cf. Sessarego, Carlos Fernández. Derecho a la identidad personal. Buenos Aires: Astrea, 1992, 141.

[31] Basan, Arthur Pinheiro, and José Luiz de Moura Faleiros Júnior. "A tutela do corpo eletrônico como direito básico do consumidor." Revista dos Tribunais, vol. 1021, 133-168, November 2020, 6.

[32] Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.' Available at: https://www.gpdp.gov.mo/uploadfile/others/wp193_pt.pdf. Access date: March 29, 2022.

[33] Article 29 Working Group for Data Protection of the European Union Opinion 4/2007 on 'Concepts of Personal Data.' Available at: https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf. Access date: March 29, 2022.

[34] Article 29 Working Group for Data Protection of the European Union Opinion 4/2007

and, in this sense, they pose risks of violations of privacy and data protection. These identifications or properties are very numerous, since someone can be identified based on many personal characteristics. The traditional - and most widely used - are concentrated in digital, iris and facial features. Genetic data also allows personal identification and has been used for a long time for recognition of filiation, which means that genetic data can also identify the owner's relatives, depending on the context (and degree).[35] Opinion 3/2012 points out, in summary, two major groups of biometric techniques: a) physical and physiological, whose examples are: fingerprint image, iris and retina recognition, face, hand, ear shape, voice, DNA and skin pores; b) behavioral, which focuses on the person's behavior, such as handwriting, gait analysis, and even lie detection patterns.[36]

The knowledge about the processes involved in biometric personal data processing becomes important as it becomes possible to identify risks to privacy and personal data protection and vulnerable data owners. The processes[37] are divided into: a) "biometric enrollment": which seeks to extract the biometric data, "from a biometric source and associate it with some person". The point of attention pointed out by Opinion 3/2012 is to collect data that is sufficient to identify the individual, without "recording excessive data". Also, not making errors in data association with the person, which would harm the data quality; b) "biometric storage": when the data remains in the reader, in an "intelligent card" that the owner carries, or, still, remotely sent to a cloud. Risks are present in terms of data security and privacy. In view of these complexities, it is necessary to monitor and evaluate the application of biometrics, to ensure their responsible and ethical use, without infringing on privacy and the protection of personal data. Risks are present in the field of information security, whether due to improper use or data leak incidents; c) "biometric correspondence": where a comparison is made between the "biometric data/model" collected at registration and the "biometric data/models collected from a "new sample". This is what happens in the case of biometrics applied to a turnstile, when the holder previously collected his/her photo/face (registration), which was recorded (stored) and every time he/she passes through the device, the user stops in front of a camera (new sample) and the comparison is made. If the comparison

on 'Concepts of Personal Data.'

[35] Among the lesser-known means is biometrics based on the measurement of the electric current in the human body, via radiometric analysis of the impedance of the fingers, cf. Noh, Hyung Wook, et al. "Ratiometric Impedance Sensing of Fingers for Robust Identity Authentication." Sci Rep 9. https://www.nature.com/articles/s41598-019-49792-9. 2019.

[36] Article 29 Working Group for Data Protection of the European Union Opinion 4/2007 on 'Concepts of Personal Data.'

[37] Article 29 Working Group for Data Protection of the European Union Opinion 4/2007 on 'Concepts of Personal Data.'

concludes with coincidence, the turnstile opens, otherwise, it doesn't.[38]

Furthermore, the specific effects or objectives to be achieved in biometrics are: "identification, verification/authentication, or categorization."[39] In "biometric identification," biometric data of a person (when registering) are compared with "a certain number of models stored in the database," which is referred to as "one to many."[40] In "authentication," the data of a single person is compared with a single model on the device. Lastly, in "categorization/separation," the essential is not its identification, but to classify the person into a certain group. For example, separating between men and women, children and adults.[41]

As it can be seen, in the realm of sensitive data, there is a diversity of possibilities of links with its holder, such data can reflect different aspects of their personality. Some of them are connected with "spiritual" aspects, while others, biometrics, directly reflect their bodily properties. In this sense, biometric data allows - or delivers to systems - a level of holder's identify virtually absolute (in some cases completely absolute, such as genetic data or fingerprints). In this sense, they tend to be immutable, as with genetic data and fingerprints mentioned above. Thus, biometric data is understood as sensitive, since it involves a higher potential for discrimination and, when facing incidents, has the ability to affect the data subjects.

At the same time, it should not be forgotten that the uses of biometric data can go beyond just establishing a unique identification in systems that perform authentication and authorization of people. The current computational power, linked to artificial intelligence techniques and pattern recognition - combined with high-resolution cameras - allow biometrics to go further. It is possible to recognize moods, emotions, humor, etc. In this sense, the possibilities and risks are expanded, allowing for the invasion of a deep sphere of the intimacy of individuals. This is what Opinion 3/2012 characterized as psychological type biometric techniques.[42]

Therefore, the connection between biometric data and the concept of the electronic body is blatant. It is about establishing a kind of very intense

---

[38] Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.' Available at: https://www.gpdp.gov.mo/uploadfile/others/wp193_pt.pdf. Access date: March 29, 2022.

[39] Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.'

[40] Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.'

[41] There is also reference to multimodal biometrics, when there is a combination of different techniques, cf. Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.'

[42] Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.'

connection with the holder, as is done with the physical body. It is important to note that a personal data may or may not be considered biometric depending on the technique used. A photo of someone in a registration system, for example, is personal data, but not necessarily biometric if biometric recognition techniques are not applied. The same photo stored in a database that allows identification through biometric recognition techniques in a banking app, for example, becomes a sensitive-biometric data by the context in which it is used. In the same vein, voice, which may be considered just personal data when the software only collects linguistic elements, that is, it only identifies the words used, differently, from cases where it uses paralinguistic elements such as tone and breathing, for example.[43]

Rodotà, in his reflections on the electronic body, also comments on the issues of biometrics. He says that given the possibilities of "identity theft", in identification and authentication processes only mediated by passwords, "alarming derivatives are emerging, which manifest themselves, particularly, through the increasingly massive use of biometric data, mainly fingerprints, thus allowing the realization of general controls on all citizens".[44] On the one hand, there would be a legitimate and justifiable possibility of using biometrics for authentication processes, on the other hand, it opens up a flank for a potentially dangerous surveillance.

The LGPD allows, and its article 11, inc. II, paragraph g), the use of biometric data for "identification and authentication processes", with the reservation that they cannot be used, on the other hand, "in the case of fundamental rights and freedoms of the holder that require protection of personal data". This means that it would not be in any situation that biometric data can be used for identification and authentication processes.[45]

Moreover, it is strange to see the naturalness with which these means are used in absolutely basic circumstances[46], where other means could be used instead of biometrics. See, for example, the cases of gymnasiums, which

---

[43] France. Commission Nationale de L'Informatique et des Libertés. "On the Record: Exploring the Ethical, Technical and Legal Issues of Voice Assistants." https://www.cnil.fr/sites/default/files/atoms/files/cnil_white-paper-on_the_record.pdf. Accessed Jan. 29, 2023.

[44] Rodotà, Stefano. "Transformações do Corpo."..., 92-93: "O corpo torna-se um instrumento para recrudescer as medidas de segurança, em uma progressão em que também a mente logo será capturada, através da invasão tentacular das tecnologias da vida cotidiana".

[45] Rodotà, Stefano. "Transformações do Corpo."..., 98: "Encontramo-nos, de fato, em terreno onde a presença de valores como os da liberdade pessoal, integridade e dignidade impede de agir como se a necessidade de segurança ou a finalidade da eficiência pudessem prevalecer sobre qualquer outra consideração".

[46] As also noted by Rodotà, when he comments on the trivialization of the use of biometric data "to the point of wanting to adopt this resource to control entry into classrooms and children's cafeterias in primary schools", cf. Rodotà, Stefano. "Transformações do Corpo."..., 93.

frequently use biometrics for access to their facilities. In such cases, and given the simplicity of the service, it is possible to use equally secure identification means, other than biometrics. One can think of a two-factor authentication, using the user's own cell phone. Note that the controller who wants to use biometrics for authentication processes must, besides respecting the principles, also surround himself with all the information security safeguards to protect these sensitive data.

Having made these considerations, we will move on to the principle analysis, and finally present recommendations for the case of the São Paulo Metro.

II. PRINCIPLES OF PURPOSE AND NECESSITY AND RECOMMENDATIONS FOR THE CASE OF THE SÃO PAULO METRO

A. Some thoughts on the Principle of Purpose and Necessity Applicable to Biometrics

The LGPD, in its article 6, establishes its philosophical basis, and, especially, for the present study, methodologically, one starts from the perspective of two principles: purpose and necessity. The principle of purpose is in article 6, I, which defines it as: "carrying out the treatment for legitimate, specific, explicit and informed purposes to the holder, without the possibility of subsequent treatment in an incompatible manner with these purposes." Arthur Pinheiro Basan well summarizes its concept, in the sense that "the purpose deals with respect for the reason why the data was collected and why it is undergoing treatment," and emphasizes the prohibition of "secondary use of data, done in an unknown and unauthorized manner by the data subject."[47] In turn, necessity is the "limitation of the treatment to the minimum necessary to achieve its purposes, with coverage of relevant, proportional and non-excessive data in relation to the data treatment purposes." It should be noted that biometric data, given the fact that they tend to be immutable, in its source, deserve special protection, especially in observance of the data protection principles highlighted.

In the theme in question, one of the main problems lies in the subsequent use (with different purposes) of biometric data collected and treated exclusively for authentication means. Rodotà points out the critical fact that genetic data, as biometric data, would have the potential to reveal information also from their relatives. According to the author, "through the genetic data of a single person, the genetic data of an entire biological group is

[47] Basan, Arthur Pinheiro. "Artigo 6º." In Comentários à Lei Geral de Proteção de Dados Pessoais, edited by Guilherme Magalhães Martins, José Luiz de Moura Faleiros Júnior, and João Victor Rozatti Longhi. Indaiatuba: Editora Foco, 2022, 60.

appropriated."[48] As seen, there is not an absolute freedom for the treatment agents to use biometric data in any circumstance that involves the identification and authentication of people. One should always consider whether the activity in question can be carried out without the use of biometric data. And this weighing should take into account the environment in which access is being made.[49] The protection of one's own assets, in the face of biometric authentications in banking environments, in the hostile environment of Internet insecurity, in principle, justifies its use. However, access to gyms does not seem to contain a degree of protection adequate to allow the use of biometric data for such access. The certainty of identification in digital systems is not a more valuable value than the protection of personal data. As Rodotá, "a compatibility test with the values of freedom and democracy to which all use of biometric data must be submitted should be performed [...] in any case, an assessment of privacy impact is always indispensable."[50]

The Opinion 3/2012, on "the evolution of biometric techniques," in its "legal analysis," deals with the importance of the principles of purpose and minimization (corresponding to necessity, in LGPD). Regarding the principle of purpose, it points to clear definition of the reason for collecting and processing biometric data as a "previous condition." Furthermore, it states that the use of biometrics must always observe a legal basis for processing, such as authorization (consent under the LGPD). Additionally, it must be highlighted that data collected for a specific purpose and in the context of a consent form cannot later be used for further processing with biometric techniques for a new purpose without specific authorization.[51]

As for the principle of minimization (necessity), the opinion emphasizes that "many times biometric data contains more information than necessary for matching functions." Therefore, in this sense, "this means that only necessary information and not all available information should be processed, transmitted, or stored." The opinion also refers to Opinion 3/2012, which states that the principle of proportionality, which in Brazil is an integral part of the principle of necessity, presents four aspects to be weighed[52]:

When analyzing the proportionality of a proposed biometric system, it

---

[48] Rodotà, Stefano. "Transformações do Corpo."..., 94.

[49] Since authentication is not an end in itself, cf. Kent, Stephen T., and Lynette I. Millett. Who Goes There? Authentication Through the Lens of Privacy. Washington: National Research Council, 2003, 2.

[50] Rodotà, Stefano. "Transformações do Corpo."..., 99.

[51] Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.' Available at: https://www.gpdp.gov.mo/uploadfile/others/wp193_pt.pdf. Access date: March 29, 2022.

[52] Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.'…

> must be considered beforehand whether the system is necessary to meet the identified need, that is, whether it is essential to meet this need and not the most practical or the one with the best cost-effectiveness. A second element to be taken into account is the likelihood of the system being effective in meeting this need due to the use of specific biometric technology. A third aspect to consider is whether the loss of privacy resulting from this is proportional to the expected benefits. If the benefit is relatively insignificant, namely a greater convenience or a slight reduction in costs, then the loss of privacy is not adequate. The fourth aspect to be taken into account in evaluating the adequacy of a biometric system is to ask if there are less invasive means that allow achieving the desired goal.[53]

From this foundation, the case of the São Paulo Metro will be analyzed, with its specificities.

B. Recommendations for the São Paulo Subway Case

This is the analysis of the Public Civil Lawsuit under number 1010667-97.2022.8.26.0053, brought by the Public Defender of the State of São Paulo, the Public Defender of the Union, IDEC - Brazilian Institute of Consumer Protection, Intervozes - Brazilian Collective of Social Communication, and Artigo 19 Brasil, against the São Paulo Subway (Companhia do Metropolitano de São Paulo), which concerns the use of facial biometrics in its facilities. Based on the PCA, it was reported that there was a bidding process for the purchase of a biometrics solution and, according to the information obtained, the system was contracted and effectively put into operation. The arguments brought against the implementation of the system, among others, are: lack of transparency in the treatment of personal data; failure to produce a Personal Data Protection Impact Report; abusive and disproportionate use of data (which implies a violation of principles); lack of parental consent for the treatment of children's data (and still the disregard of the preservation of their best interests). In addition, it was argued that facial recognition systems would be more flawed for black and LGBTQIA+ people (with serious identification errors and algorithmic discrimination). These issues were pointed out by Professor Roberto Hirata Jr., who also highlighted the "absence of information [...] capable of demonstrating the mitigation of the risks presented by the system to subway users" and the "absence of indication of the database to be used by the subway to train facial recognition models, even though such information is of great importance to evaluate the

[53] Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.'…

efficiency of the project." The same professor also points out other features that the SecureOS system of the Russian company ISS would have, such as: "detection of a person running; detection of crowds; detection of people stopping for more than a certain amount of time in a certain place," etc. Also, according to the PCA, the images will be stored (of all users) and the system could still be connected to other monitoring systems.

One of the issues to be discussed is the uncertainty about the purpose of using the facial recognition system. In terms of the ACP, the Metro would intend to use the system for "detection of perimeter invasions, object tracking, facial recognition and others, with a view to preventing criminal offenses and increasing passenger safety" and about the facial recognition capabilities. Its use would also be for "searching for missing persons, or identifying a user who may have committed a crime on the premises of the Metro, as well as search after judicial determination". It should be noted that there are several purposes, which, depending on the case, require different concerns about the protection of personal data. The Metro, in addition, stated that "processing or monitoring of personal data" would not be performed. However, this argument is not sustained, as the information based on each person's face that allows for their subsequent recognition is not only personal data, but sensitive personal data, as it is biometric (cf. article 5, item II of the LGPD). Since recognition can be subsequent, the ACP also points out that there would be a blatant disproportionate system as a whole, since the image of all people passing through the stations would be stored to allow for future consultations and identifications. There are also doubts about the information security measures to be taken in managing biometric data.[54]

The use of surveillance technologies is one of the major issues addressed in the field of data protection worldwide.[55] Concerns range from the potential violation of the law, when surveillance is carried out in contravention of the legal order, but also touch on social issues, when the impact and its effect on the population of a certain location are investigated.[56] The objective is to

[54] Given the nature of such data, security measures must be expanded, adopting not only the principle of privacy by design, but security by design. Brief safety instructions can be found in Welinder, Yana and Areyn Palmer. "Face Recognition, Real-Time Identification, and Beyond." In The Cambridge Handbook of Consumer Privacy, edited by Evan Selinger, Jules Polonetsky, and Omar Tene. Cambridge: Cambridge University Press, 2018, 124.

[55] Without forgetting the reflections of Jeremy Bentham in his panopticon (analyzed by Foucault in his Discipline and Punish), still in the 18th century, currently seen as the “most powerful metaphor in pointing out the theoretical and social significance of CCTV mechanisms in society contemporary”, (our translation), cf. Norris, Clive. "CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control." In Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination, edited by David Lyon, London: Routledge, 2003.

[56] One of the most relevant authors in the modern analysis on the subject is Lyon, David. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota

analyze how surveillance means can serve as a form of social control[57], affecting, for our purposes here, informational self-determination and the free development of personality.

The use of facial recognition is not prohibited by the LGPD, however, the system must undergo a test of compliance with the legal order, evaluating its functionalities, the specific activities involved, and solutions must be proposed based on the case, not based on abstract scenarios, or "all or nothing" decisions. The answer to the question of the possibility of its use in the analyzed context first requires the verification of the existence of at least one of the authorizations for the processing of personal data. In this case, facial recognition is classified as sensitive data due to its biometric nature. Thus, for the proper evaluation, it is necessary to examine the assumptions of article 11 of the LGPD.[58] In this way, the first assumption would be consent, which does not exist and would also be impractical, given the large number of people who use the service.[59] It is true that, with the specific and separate consent of the service user, facial recognition could be allowed for the specific purpose of, for example, controlling passages. This would be the case of biometrics consented to authenticate the user at the time of identifying him or her to pass through turnstiles. It should be noted that, in this situation, consent must always be linked to the purpose. Currently, in the case at hand, there is no consent. It should also be noted that the means of identification and authentication should always be perceived by the data holder or whether

---

Press, 1994. Also, regarding surveillance as "social sorting", cf. Lyon, David. "Surveillance as Social Sorting: Computer Codes and Mobile Bodies." In Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination, edited by David Lyon. London: Routledge, 2003, 13 *et seq*. Other concerns occur in the possibility of evolution of means of surveillance and how they can become means of predictive policing, according to the concern (and indication of consequences) of O'Neil, Cathy. Weapons of Math Destruction: How big data increases inequality and threatens democracy. New York: Crown, 2016, 86-87.

[57] Rodotà, Stefano. Il diritto…, 90: "Politiche di sicurezza pubblica e logiche di mercato dispongono oggi di mezzi di ampiezza senza precedenti, che permettono loro di impadronirsi d'ogni sfaccettatura della vita d'ogni persona, di «depersonalizzarla» attraverso la negazione dell'unicità e la riconduzione di ciascuno a un «profilo»".

[58] It should be noted that this is the hypothesis for the treatment of biometric data. The treatment of data of another nature, naturally, can be carried out by different treatment hypotheses.

[59] In fact, the Danish Data Protection Agency has already positioned itself to indicate that it is a violation of the RGPD the use of facial recognition mechanisms to access a company for those who do not give their consent, which, in practice, would be the same as prohibiting its use in this context. Cf. Denmark. Datatilsynet. "Datatilsynet Has Made a Decision in a Case Regarding the Use of a Face Recognition System." Available at: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse. Accessed Jan. 29, 2023.

it is a "transparent" means that identifies them without their knowledge.[60] Explained: when someone puts their finger on a fingerprint reader, they perceive and recognize that there is a form of recognition of their fingerprint; on the other hand, if the system is done through recorded images, most people will not even realize that recognition is being done. This differentiation, between the use of biometrics with or without the participation of the data subjects, must be observed, especially in the context of compliance with the principle of transparency, since the data holder does not even realize that the processing of their biometric data is being carried out.

Regarding the hypotheses related to legal and regulatory obligations, it is understood that the justification brought by the Public Defender is correct, since there is no law or regulatory norm that determines, in a compelling manner, the collection of biometric data by the subway, for the purposes practiced by it. For the achievement of conclusions on the subject, a careful analysis of the end activities and services made available by the mentioned public company is unavoidable. The fact of being a public company does not allow it to carry out acts of public security, therefore, it would not be equivalent in this point to the State itself. It should be noted that the doctrine[61] also considers that the processing of data through monitoring cameras in public environments, with facial recognition for the identification of sought persons, would be a treatment in the scope of public security, therefore, the LGPD would not apply.

Regarding the use of data for public policies, it is important to mention that recent jurisprudential history has already established the criteria for the use of data by the public administration, in the terms of the joint judgment, in a preliminary manner, of the Direct Actions of Unconstitutionality (ADI) under numbers 6387 to 6390 and 6393, with the Supreme Federal Court. The Supreme Court determined that the public administration, to access and treat citizens' personal data, must observe the application of the "classical principles of data protection"[62], such as the principle of purpose,

---

[60] Cf. Kent, Stephen T., and Lynette I. Millett. Who Goes There?..., 46: “Some biometrics, on the other hand, can be used to identify individuals without those individuals’ active participation and awareness, so care needs to be taken when using biometrics in authentication systems designed to ensure accountability”.

[61] Abreu, Jacqueline de Sousa. "Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD." In Tratado de Proteção de Dados Pessoais, edited by Danilo Doneda et al. Rio de Janeiro: Gen/Forense, 2020, 591. It should be remembered that this was just one of the purposes indicated by the Metro. The preliminary draft of the Criminal LGPD should be highlighted, which addresses such issues, including the requirement of a “surveillance impact report” due to high risk situations for data subjects.

[62] Doneda, Danilo. "Registro da Sustentação Oral no Julgamento da ADI 6389, sobre a Inconstitucionalidade do Art. 2º, Caput e §§ 1º e 3º da MP 954/2020." Civilistica.com, vol. 9, no. 1, 2020. https://civilistica.emnuvens.com.br/redc/article/view/519/397. Accessed Jan. 29, 2023.

transparency, security, proportionality and the principle of minimization.[63] And, still, in line with the mentioned Guidelines, "anonymized data must always be given preference over personal data". Simply implementing biometrics, as a general rule, is an disproportionate practice, going against the principiology of protection of personal data. Thus, the application of facial recognition could be considered an excessive collection, that exceeds the implemented purposes, given the possibility of using video surveillance through filming.[64] On the other hand, the identification measures carried out in the airport environment, for example, cannot be compared because they are related to activities carried out by the government and federal revenue (identification for access to the boarding room and aircrafts). The controls carried out in this environment (by the Revenue and even the Federal Police) do not compare with the activities and needs of a subway or other means of transportation other than civil aviation. At the same time, it must be emphasized that the air transport contract requires the adequate and secure identification of passengers, which does not occur with other modes of transport.[65]

Security could be offered to users by recording the image and, upon judicial order, applying facial recognition to the records afterwards[66], in order to prevent unreasonable and widespread exposure of people. As correctly pointed out in the ACP, there is still the issue of potential discrimination, but it is indeed recognized as possible by specialized doctrine.[67]

Regarding article 11, II, "g", it can be inferred that it would be possible to use personal data without consent for "ensuring the prevention of fraud and

---

[63] Colombo, Cristiano and Wilson Engelmann. "Inteligência Artificial em favor da saúde: proteção de dados pessoais e critérios de tratamento em tempos de pandemia." In Inteligência Artificial aplicada ao processo de tomada de decisões, edited by Henrique Alves Pinto, Jefferson Carús Guedes, and Joaquim Portes de Cerqueira César, v. 1, 225-246. Belo Horizonte: D'Plácido, 2020, 225-246. It should also be remembered that the general principles applied to the present case, such as adequacy and necessity, also help to control the risk of deviations from purposes in the use of biometric data, one of the greatest risks in such contexts, especially in the face of deviations promoted by the state, cf. Lodge, Juliet. "Nameless and Faceless: The Role of Biometrics in Realizing Quantum (In)security and (Un)accountability." In Security and Privacy in Biometrics, edited by Patrizio Campisi. London: Springer, 2013, 329.

[64] It is totally possible to use video surveillance means that do not involve the collection or processing of data for facial recognition purposes of any kind. It is even possible to implement a system that automatically blurs people's faces, as with Google Street View.

[65] Enerstved, Olga Mironenko. Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles. Cham: Springer, 2017, 226.

[66] Specific analysis about the processing of personal data in the criminal context is still needed for proper conclusions to be drawn.

[67] Kuipers, Benjamin. "Perspectives on Ethics of AI." In The Oxford Handbook of Ethics of AI, edited by Markus D. Dubber, Frank Pasquale, and Sunit Das. Oxford: Oxford University Press, 2020, 434.

the security of the holder, in the processes of identification and authentication of registration in electronic systems", which is understood to be fully practiced, without excess, through recordings, without facial recognition, including storage for a longer period. At this point, the second part of subparagraph "g" should lead to the conclusion that the implementation of facial recognition would result in a disproportionate imbalance between the fundamental rights and freedoms of the holder and the measures to provide security or combat frauds. It should be noted that the hypothesis of legitimate interest, which allows for an analysis of the ambiance of the contractual relationship, with the identification of the objectives and interests of the contracting parties, is excluded, as they are sensitive data, being biometric. Reflections on the importance of good practices in protecting personal data, and also the role of the data protection officer (DPO), to enforce the authorized hypotheses and mediate relationships between users, company and the National Authority for the Protection of Personal Data (ANPD), are of great importance. Finally, the biggest problem in the case of the São Paulo subway is the absolutely generalized collection of data in its dependencies[68], disregarding all the weight that biometric data represents for the constitution of the person in question.

CONCLUSION

With this work, it is sought to provide arguments for expanded protection of biometric data in the Brazilian data protection scenario. The search for the explanation of issues related to the physical body and electronic body aims to bring a potential foundation for the application of more intense controls on the use of biometric data. The use of data of this nature cannot be trivialized under penalty of violating the data subjects, even due to incidents.

Therefore, it is considered that:

a) The indiscriminate, general, and instantaneous application of facial recognition to all subway users exceeds the principles of personal data protection and is a disproportionate measure that offends the principles of necessity and minimization of data collection, since other techniques, such as security cameras in spaces without biometrics, can fully meet the security and fraud prevention purposes for their users;

b) Even so, it is necessary to carefully evaluate the purpose of the use of CCTV images, whether or not there is the collection and use of biometric data, which would shift the hypothesis of treatment to Article 11 of the LGPD, falling into the category of sensitive data. It should be noted that the

[68] Cf. Rodotà, Stefano. Transformações do Corpo…, 99, "As coletas generalizadas, de fato, sobretudo quando justificadas por razões de segurança, modificam a percepção social que delas se tem e acabam por transformar todos os cidadãos em suspeitos em potencial".

treatment of data for public security purposes is not covered by the provisions of the LGPD;

c) As a collaborative solution, recordings could be stored by the subway company and, in the concrete case, accessed through a court order, with facial recognition techniques only later being applied to the records, the procedure being in line with the principles of adequacy and necessity;

d) Facial recognition, accompanied by consent, may be used for specific purposes and in the context of the transportation service contract between the parties, for example, in the case of biometry consented to authenticate the user at the time of identifying him to pass through the turnstiles;

e) Among the solutions considered for its application, the installation of facial recognition with data storage by the state through its police forces, to be treated exclusively for public security purposes, would be suggested, in which case the limitations of the LGPD would not apply, under the terms of Article 4, III, where the data manager would have public security as its end activity, turning to these purposes. However, even so, from the analysis of the LGPD Penal draft, which is based on the principles of personal data protection, it can be inferred that, in the rule of Article 43, it is explicitly stated that "the use of surveillance technologies directly increased with techniques for identifying undetermined people in real time and continuously when there is no connection with the individualized and authorized criminal persecution activity by law and judicial decision" will not be allowed if the text under discussion is approved. This means that facial recognition cannot be a cannon pointed at a large mass of users, but, on the contrary, its application must be conducted to the particularized look, with precision and accuracy, aiming to reduce the impact on human rights, with the use of data being subjected to principles of transparency and accountability.

Furthermore, with regards to the chronological criterion, it cannot be done in real time, affecting everyone, but rather, a posteriori, focused on those described in the court order. Lastly, it is important to emphasize that best practices should be orchestrated with the right to personal data protection, as a category of fundamental right, in accordance with Constitutional Amendment 115 of 2022, which dismisses general, simultaneous, and indiscriminate facial recognition, unaccompanied by a specific court order, in favor of an individualized, well-criteria and timely tool.

The contributions brought forward aim to harmonize the use of technology in an environment attentive to privacy and personal data protection, considering biometric data as a highly expanded connection with its data subjects.

REFERENCES

Abreu, Jacqueline de Sousa. "Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD." In Tratado de Proteção de Dados Pessoais, edited by Danilo Doneda et al. Rio de Janeiro: Gen/Forense, 2020.

Almeida, José Luiz Gavião de, Luis Renato Vedovato, and Marcelo Rodrigues da Silva. "A identidade pessoal como direito fundamental da pessoa humana e algumas de suas manifestações na ordem jurídica brasileira." Revista de Direito Civil Contemporâneo, vol. 14, 33-70, January-March 2018.

Article 29 Working Group for Data Protection of the European Union Opinion 3/2012 on 'Evolution of Biometric Technologies.' Available at: https://www.gpdp.gov.mo/uploadfile/others/wp193_pt.pdf. Access date: March 29, 2022.

Article 29 Working Group for Data Protection of the European Union Opinion 4/2007 on 'Concepts of Personal Data.' Available at: https://www.gpdp.gov.mo/uploadfile/others/wp136_pt.pdf. Access date: March 29, 2022.

Basan, Arthur Pinheiro. "Artigo 6º." In Comentários à Lei Geral de Proteção de Dados Pessoais, edited by Guilherme Magalhães Martins, José Luiz de Moura Faleiros Júnior, and João Victor Rozatti Longhi. Indaiatuba: Editora Foco, 2022.

Basan, Arthur Pinheiro, and José Luiz de Moura Faleiros Júnior. "A tutela do corpo eletrônico como direito básico do consumidor." Revista dos Tribunais, vol. 1021, 133-168, November 2020.

Brazil. Chamber of Deputies. Anteproject of Data Protection Law for Public Safety, 2020. Available at https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf. Access on: March 29, 2022.

Breton, David. La sociologie du corps. 8th ed. Paris: PUF, 2012. Digital edition.

Bucar, Daniel and Teixeira, Daniele Chaves. "Autonomia e Solidariedade." In O direito Civil - Entre o Sujeito e a Pessoa: Estudos em homenagem ao professor Stefano Rodotà, edited by Gustavo Tepedino, Ana Carolina Brochado de, and Vitor Almeida. Belo Horizonte: Fórum, 2016.

Chaves, Antônio. Direito à vida e ao próprio corpo (Intersexualidade, transexualidade, transplantes). 2nd ed. São Paulo: Revista dos Tribunais, 1994.

Choeri, Raul Cleber da Silva. O conceito de identidade e a redesignação

sexual. Rio de Janeiro: Renovar, 2004.

Cifuentes, Santos. Elementos de derecho civil: Parte general. 4th ed. Buenos Aires: Astrea, 1999.

Colombo, Cristiano and Wilson Engelmann. "Inteligência Artificial em favor da saúde: proteção de dados pessoais e critérios de tratamento em tempos de pandemia." In Inteligência Artificial aplicada ao processo de tomada de decisões, edited by Henrique Alves Pinto, Jefferson Carús Guedes, and Joaquim Portes de Cerqueira César, v. 1, 225-246. Belo Horizonte: D'Plácido, 2020.

Colombo, Cristiano and Guilherme Damasio Goulart. "Nota técnica sobre o uso de biometria facial no metrô de São Paulo." Boletim da Revista dos Tribunais Online, n. 25, 1-6. São Paulo: Revista dos Tribunais Online, March, 2022.

Cupis, Adriano de. Il Diritto all'Identità Personale. Milan: Dott. A. Giuffrè, 1949.

Denmark. Datatilsynet. "Datatilsynet Has Made a Decision in a Case Regarding the Use of a Face Recognition System." Available at: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse. Accessed March 29, 2022.

Doneda, Danilo. "Registro da Sustentação Oral no Julgamento da ADI 6389, sobre a Inconstitucionalidade do Art. 2º, Caput e §§ 1º e 3º da MP 954/2020." Civilistica.com, vol. 9, no. 1, 2020. https://civilistica.emnuvens.com.br/redc/article/view/519/397. Accessed Jan. 29, 2023.

Enerstved, Olga Mironenko. Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles. Cham: Springer, 2017.

Floridi, Luciano. "The Construction of Personal Identities Online." Minds & Machines, vol. 21, no. 1, 477-79, 2011.

France. Commission Nationale de L'Informatique et des Libertés. "On the Record: Exploring the Ethical, Technical and Legal Issues of Voice Assistants." https://www.cnil.fr/sites/default/files/atoms/files/cnil_white-paper-on_the_record.pdf. Accessed Jan. 29, 2023.

Gonçalves, Diogo Costa. Pessoa e Direitos de Personalidade: Fundamentação Ontológica da Tutela. Coimbra: Almedina, 2008.

Italy. Camera dei Deputati. "Dichiarazione dei diritti in Internet." Available at https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf. Access on: March 29, 2022.

Kent, Stephen T., and Lynette I. Millett. Who Goes There? Authentication

Through the Lens of Privacy. Washington: National Research Council, 2003.

Kuipers, Benjamin. "Perspectives on Ethics of AI." In The Oxford Handbook of Ethics of AI, edited by Markus D. Dubber, Frank Pasquale, and Sunit Das. Oxford: Oxford University Press, 2020.

Lodge, Juliet. "Nameless and Faceless: The Role of Biometrics in Realizing Quantum (In)security and (Un)accountability." In Security and Privacy in Biometrics, edited by Patrizio Campisi. London: Springer, 2013.

Ludwig, Marcos de Campos. "O Direito ao Livre Desenvolvimento da Personalidade na Alemanha e Possibilidades de sua Aplicação no Direito Privado Brasileiro." Revista da Faculdade de Direito da UFRGS, vol. 19, 237-63, March 2001.

Lyon, David. "Surveillance as Social Sorting: Computer Codes and Mobile Bodies." In Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination, edited by David Lyon. London: Routledge, 2003.

Lyon, David. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press, 1994.

Marini, Giovanni. "Commento di Artt. 3-186." In Commentario del Codice Civile. Delle Persone, edited by Angelo Barb and Stefano Pagliantini, Torino: UTET, 2013.

Mota Pinto, Paulo. "O Direito ao Livre Desenvolvimento da Personalidade." In Boletim da Faculdade de Direito de Coimbra, Portugal-Brasil Ano 2000, 149-246, 1999.

Noh, Hyung Wook, et al. "Ratiometric Impedance Sensing of Fingers for Robust Identity Authentication." Sci Rep 9. https://www.nature.com/articles/s41598-019-49792-9. 2019.

Norris, Clive. "CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control." In Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination, edited by David Lyon, London: Routledge, 2003.

O'Neil, Cathy. Weapons of Math Destruction: How big data increases inequality and threatens democracy. New York: Crown, 2016.

Perlingieri, Pietro. O Direito Civil na legalidade constitucional. Translated by Maria Cristina de Cicco. Rio de Janeiro: Renovar, 2008.

Rodotà, Stefano. Il diritto di avere diritti. Rome: Laterza, 2012.

Rodotà, Stefano. Il mondo nella rete. Quali i diritti, quali i vincoli. Rome: Laterza & Figli, 2014.

Rodotà, Stefano. "Transformações do Corpo." Revista Trimestral de Direito Civil, Rio de Janeiro 19 (July-September 2004): 91-107.

Rodotà, Stefano. Vivere la democrazia. Rome: Laterza & Figli, 2018, digital edition.

Sarmento, Daniel. Dignidade da pessoa humana: conteúdo, trajetórias e

metodologia. 3rd ed. Belo Horizonte: Fórum, 2016.
Schreiber, Anderson, et al. Código Civil Comentado: Doutrina e Jurisprudência. 3rd ed. Rio de Janeiro: Forense, 2021.
Sessarego, Carlos Fernández. Derecho a la identidad personal. Buenos Aires: Astrea, 1992.
Souza, Rabindranath V.A. Capelo de. O Direito Geral de Personalidade. Coimbra: Coimbra, 2011.
Welinder, Yana and Areyn Palmer. "Face Recognition, Real-Time Identification, and Beyond." In The Cambridge Handbook of Consumer Privacy, edited by Evan Selinger, Jules Polonetsky, and Omar Tene. Cambridge: Cambridge University Press, 2018.

* * *

Cristiano Colombo
Post-Doctorate in Law, Pontifical Catholic University of Rio Grande do Sul (PUCRS). Ph.D, Federal University of Rio Grande do Sul (UFRGS). Master of Laws, Federal University of Rio Grande do Sul (UFRGS). Bachelor of Juridical and Social Sciences, Pontifical Catholic University of Rio Grande do Sul (PUCRS) and in Accounting Sciences, Federal University of Rio Grande do Sul (UFRGS). Specialist in Tax Law, Brazilian Institute of Tax Studies (IBET). Completed the Advanced Formation Course of the Social Studies Center of the Laboratory Associated with the University of Coimbra (Portugal) named: "Cyberspace: Challenges to Justice". Professor of the Professional Master's Degree Program in Business and Law at University of Vale dos Sinos (UNISINOS), Professor of undergraduate courses in Law, Foreign Trade and International Relations at University of Vale dos Sinos (UNISINOS) and at the Law School of São Judas Tadeu Integrated Colleges. Coordinator of the LLM in General Law for the Protection of Personal Data. FAPERGS Researcher. Was a member of the Legal Education Commission (CEJ) of the Order of Lawyers of Brazil of Rio Grande do Sul.
Email: cristianocolombo@unisinos.br
ORCID iD: https://orcid.org/0000-0002-4362-0459

Guilherme Damasio Goulart
Ph.D (2020) and Master of Laws, Federal University of Rio Grande do Sul (UFRGS). Lawyer, professor, and consultant in Information Security, Technology Law, and Personal Data Protection. Has taught classes, lectures, and seminars on Technology Law and Information Security at institutions such as Ulbra, Uniritter, UFRGS, UCS, IPA-Metodista, Setrem, FEMA, Brazilian Internet Steering Committee (CGI.br), and also at the School of the Attorney General's Office (AGU). Internationally, he participated as a professor in the IV-Luso-Brazilian Course in Electronic Law and the Luso-Brazilian Journeys of the Center for Private Law Research (CIDP) both at the Faculty of Law of the University of Lisbon (Portugal). He is a visiting professor in the Specialization Course in Consumer Law and Fundamental Rights and was a professor in the Specialization Course in International Law, both at UFRGS. He is a professor in the post-graduations of Damasio Educacional, SENAC-RS and Verbo Jurídico, teaching subjects related to Cyberlaw, Civil Liability in Computer Science and Information Security.
Email: guilherme@direitodatecnologia.com
ORCID iD: https://orcid.org/0000-0001-6724-9335

10.59224/bjlti.v1i1.1-22
ISSN: 2965-1549