BIOMETRIC DATA: AN ANALYSIS OF BILL 2338/2023 BASED ON THE PARAMETERS ESTABLISHED IN THE EUROPEAN UNION AI ACT

DADOS BIOMÉTRICOS: UMA ANÁLISE DO PROJETO DE LEI 2338/2023 A PARTIR DOS PARÂMETROS ESTABELECIDOS NO AI ACT DA UNIÃO EUROPEIA

DATOS BIOMÉTRICOS: UN ANÁLISIS DEL PROYECTO DE LEY 2338/2023 A PARTIR DE LOS PARÁMETROS ESTABLECIDOS EN EL AI ACT DE LA UNIÓN EUROPEA

https://doi.org/10.56238/sevened2026.008-058

Joaquim Ribeiro de Souza Junior[1], Glenda Almeida Matos Moreira[2]

ABSTRACT

This article analyzes how biometric data and biometric systems are regulated in Brazil's Bill of Law No. 2,338/2023 (the proposed Brazilian AI framework) in light of the standards set by Regulation (EU) 2024/1689 (the AI Act). It starts from the premise that biometrics, although classified as sensitive personal data under the LGPD, has expanded rapidly in Brazil across public and private settings, notably through state identification infrastructures and facial recognition deployments in publicly accessible spaces. Such uses have fueled controversy due to error rates, bias, and discriminatory impacts. Using a qualitative, documentary approach, the study outlines core operational concepts (biometric identification, verification/authentication, remote biometric identification, emotion recognition, and biometric categorization), summarizes the AI Act's risk-based architecture (prohibited practices, high-risk requirements, and safeguards for real-time remote biometric identification), and then examines the bill's main biometric provisions. The comparison shows a shared regulatory backbone: a general ban on real-time remote biometric identification in publicly accessible spaces with narrowly defined exceptions, coupled with stronger governance, transparency, and impact-assessment duties for high-risk uses. At the same time, the article identifies gaps and improvement paths for the Brazilian bill inspired by the AI Act, including: more granular procedural safeguards and independent oversight for exceptions; audit trails and clear deletion duties; an explicit prohibition on building or expanding facial databases through untargeted scraping; a clearer framework for 'post' remote biometric identification (ex post searches); and more specific limits on biometric categorization and emotion recognition in asymmetric environments such as workplaces and educational institutions. The article concludes that the EU framework offers actionable parameters to strengthen fundamental-rights protection and accountability in biometric AI deployments in Brazil.

Keywords: Biometric Data. Remote Biometric Identification. Facial Recognition. Bill 2,338/2023. EU AI Act. Risk-Based Regulation.

[1] Doctoral student in Law. Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
E-mail: joaquimjunior33@gmail.com Orcid: https://orcid.org/0000-0003-3488-5508

[2] Doctoral student in Law. Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Centro Universitário. E-mail: glendaalmeidamoreira@gmail.com Orcid: https://orcid.org/0000-0002-8940-3644

RESUMO

O artigo examina o tratamento jurídico dos dados e sistemas biométricos no Projeto de Lei nº 2.338/2023 (marco brasileiro de inteligência artificial) à luz dos parâmetros do Regulamento (UE) 2024/1689 (AI Act). Parte-se da constatação de que a biometria, embora enquadrada como dado pessoal sensível pela LGPD, vem sendo amplamente utilizada no Brasil em serviços públicos e privados, especialmente em infraestrutura estatal de identificação (por exemplo, bancos civis e sistemas como AFIS/ABIS) e em aplicações de reconhecimento facial em espaços públicos, cenário que tem gerado controvérsias por erros, vieses e impactos discriminatórios. A pesquisa, de caráter qualitativo e documental, descreve conceitos operacionais (identificação biométrica, verificação/autenticação, identificação biométrica remota, reconhecimento de emoções e categorização biométrica), apresenta as principais escolhas regulatórias do AI Act (regulação por risco, práticas proibidas, requisitos para sistemas de alto risco e salvaguardas para identificação biométrica remota em tempo real) e, em seguida, analisa o PL 2338/2023, com foco na vedação, como regra, da identificação biométrica à distância em tempo real em espaços acessíveis ao público, nas hipóteses de exceção e nas obrigações de governança, transparência e avaliação de impacto algorítmico para usos no setor público. O cotejo revela convergência estrutural entre os modelos (proibição com exceções tipificadas e regime reforçado para alto risco), mas também aponta lacunas e oportunidades de aprimoramento no projeto brasileiro: detalhamento de salvaguardas e supervisão externa para exceções, trilhas de auditoria e deveres claros de descarte; proibição expressa de formação/expansão de bases faciais por raspagem não direcionada; disciplina mais densa para identificação biométrica remota "posterior" (ex post); e limites específicos para categorização biométrica e para reconhecimento de emoções em contextos assimétricos, como trabalho e educação. Conclui-se que os parâmetros europeus oferecem referências concretas para fortalecer a proteção de direitos fundamentais e a responsabilização no uso de biometria mediado por IA no Brasil.

Palavras-chave: Dados Biométricos. Identificação Biométrica Remota. Reconhecimento Facial. PL 2338/2023. AI Act. Regulação por Risco.

RESUMEN

El artículo analiza el tratamiento normativo de los datos y sistemas biométricos en el Proyecto de Ley nº 2.338/2023 (marco brasileño de inteligencia artificial) a partir de los parámetros del Reglamento (UE) 2024/1689 (AI Act). Se parte de que la biometría, aunque es dato personal sensible en la LGPD, se ha expandido en Brasil en ámbitos públicos y privados, en especial en infraestructuras estatales de identificación y en el reconocimiento facial en espacios de acceso público, con controversias por errores, sesgos e impactos discriminatorios. Con metodología cualitativa y documental, el estudio delimita conceptos operativos (identificación biométrica, verificación/autenticación, identificación biométrica remota, reconocimiento de emociones y categorización biométrica), sintetiza el enfoque de regulación por riesgo del AI Act (prácticas prohibidas, obligaciones para sistemas de alto riesgo y salvaguardas para la identificación remota en tiempo real) y contrasta esas categorías con la disciplina propuesta en el PL 2.338/2023. La comparación muestra convergencias: prohibición general de la identificación biométrica remota en tiempo real en espacios accesibles al público con excepciones tipificadas y deberes reforzados de gobernanza y transparencia. Asimismo, identifica mejoras posibles inspiradas en el AI Act: mayor detalle de salvaguardas y supervisión independiente para las excepciones (trazabilidad y deberes de eliminación), prohibición expresa del raspado no dirigido para crear o ampliar bases faciales, tratamiento claro de la identificación remota "posterior" (ex post) y límites específicos para categorización biométrica y reconocimiento de emociones en contextos asimétricos como trabajo y educación.

Palabras clave: Datos Biométricos. Identificación Biométrica Remota. Reconocimiento Facial. PL 2338/2023. Ley de IA. Regulación por Riesgo.

1 INTRODUCTION

The expansion of the use of biometric data and biometric systems in Brazil appears in institutional registries and in the literature as a phenomenon associated with the identification and verification of identity in public and private contexts, with applications in public security, access control to services, and digital transactions.

This dynamic inserts biometrics into technical arrangements that depend on the automated collection, storage, and comparison of physical, physiological, or behavioral characteristics, which expands the role of data infrastructures and decision-making mechanisms based on computational models.

In the Brazilian legal field, biometric data appear as sensitive personal data in the General Data Protection Law (LGPD), which conditions its processing to specific legal hypotheses and duties to observe principles such as purpose, necessity, and transparency.

However, in this context there are public controversies about the use of biometric surveillance and with records of errors, biases and social contestation, especially in facial recognition applications in public spaces and in private practices of exposing images of suspects.

Recently, the European Union approved Regulation (EU) 2024/1689, known as the AI Act, which structures a risk-based regulation regime for artificial intelligence systems and includes specific discipline for biometric uses, with prohibitions, operational categories, and procedural requirements, especially for real-time remote biometric identification in publicly accessible spaces.

In Brazil, the discussion on an artificial intelligence framework was consolidated in Bill No. 2338/2023 (PL 2338), which proposes a risk classification regime, governance duties, and instruments such as algorithmic impact assessment, in addition to bringing operational definitions of biometric identification and biometric authentication and specific discipline for remote biometric identification in real time in spaces accessible to the public, with a prohibition rule and exception hypotheses.

This article analyzes the normative treatment of biometrics in PL No. 2338/2023 based on the parameters of the AI Act, focusing on remote biometric identification, authentication, emotion recognition, and other biometric uses that involve surveillance, categorization, and decision-making mediated by AI systems. The investigation adopts a qualitative and documentary approach, with a comparative examination of provisions of the PL and the AI Act, in addition to reading institutional materials and literature used to contextualize uses and controversy.

Based on this approach, the text seeks to identify regulatory convergences and gaps in the discipline of biometrics, with special attention to procedural safeguards, transparency duties, and accountability mechanisms associated with the use of biometric systems in public and private contexts.

The structure of the article starts from a conceptual contextualization of biometrics and biometric systems and their uses in Brazil, including national normative parameters and recent controversies, and then describes the central elements of the AI Act on biometrics. Next, it examines PL No. 2338/2023 with a focus on its biometric provisions and compares the regimes, to formulate a synthesis of the convergences and normative perspectives that emerge from the comparison between the two regulatory matrices and, then, demonstrate the perspectives of the AI Act for Brazilian law.

2 BIOMETRICS AND ARTIFICIAL INTELLIGENCE

In the context of human identification, biometrics can be understood as a set of techniques that establish a person's identity based on physical and behavioral attributes, using statistical, biological and technological methods and based on the capture of personal data.

Biometric data, in turn, are personal data resulting from specific technical processing related to physical, physiological or behavioral characteristics, capable of allowing or confirming the unique identification of the holder, with examples such as facial images and dactyloscopic data, which can serve the authentication, identification or classification of people, with use by both companies and governments (Silva, 2023).

In this sense, part of the literature differentiates biometrics as a technical field and biometric data as the product of a technical processing on a characteristic, which brings the debate on data governance closer, as the body trait starts to circulate as information that can be operationalized by machines and third parties (Silva, 2023).

The definitions adopted by Brazil (2019) are also highlighted. Decree 10,046/2019 differentiates biographical data — those related to facts of the person's life, such as civil or social name, date of birth, parentage, place of birth, nationality, sex, marital status, family group, address, and employment relationships —, and biometric data, measurable biological and behavioral characteristics, collectible for automated recognition, such as palm of the hand, fingerprints, retina or iris, face shape, voice and way of walking.

According to Violato et. al (2013), biometric systems operate from these characteristics for automated recognition. They usually use sensors to capture the characteristic, produce a biometric model and store it in a database, which enables future comparisons to identify or verify individuals in concrete situations. Biometric recognition systems tend to include a training stage with real samples, in which the quality and representativeness of the training base are associated with the performance of the system in the target population.

This area has recently been increased with Artificial Intelligence, thus enabling the extension and efficiency of these systems. Facial recognition, for example, is an application of artificial intelligence that uses biometric collection based on facial features. This process occurs by measuring points on the face and extracting biometric data that enables verification and authentication, with the transformation of these measurements into numerical representation and frequent storage for future comparisons (Baccarin, 2023).

As Silva (2023) points out, capture usually occurs by digital cameras integrated with software with artificial intelligence algorithms that analyze the image, measure characteristics, and produce a stored biometric model for feedback to the system, which can occur in real time and on an expanded scale according to the technical arrangement implemented.

Thus, in terms of result, there is a description that facial recognition operates by similarity and by probability judgment, which means that the output of the system does not correspond to the right answer, but to the most likely match within the compared set, with the occurrence of false negatives and false positives influenced by factors such as background and lighting.

The use of facial recognition can also be articulated with profiling practices, with the creation of digital profiles based on information collected and with the possibility of categorization by attributes, which expands the circulation of biometric data beyond the initial act of authentication (Doneda, 2006 apud Silva, 2023).

2.1 BRAZILIAN NORMATIVE PARAMETERS ON THE USE OF BIOMETRICS

In Brazil, biometric data are part of the category of sensitive personal data, which subjects its processing to specific requirements and its own legal hypotheses (ANPD, 2025). The ANPD notes that the LGPD did not define biometric data, and that part of the doctrine uses the description of the GDPR, in which biometric data results from technical treatment related to physical, physiological, or behavioral characteristics that allow or confirm unique identification.

The processing of biometric data, while sensitive, must be based on the hypotheses of article 11 of the LGPD, with the provision of specific and detached consent, or databases without consent linked to delimited purposes, such as legal obligation, public policies, studies, exercise of rights, protection of life, protection of health and prevention of fraud and security of the holder in identification and authentication processes in electronic systems (Baccarin, 2023).

In the same section, there is a record that sensitive data cannot be processed based on legitimate interest or credit protection, which restricts alternatives frequently used for non-sensitive data.

In private and public delegated applications, part of the literature emphasizes subparagraph "g" of article 11, which admits the treatment for fraud prevention and security of the holder in processes of identification and authentication of registration in electronic systems, with express exception regarding the prevalence of fundamental rights and freedoms of the holder and with requirements for information on purposes and storage time (Silva, 2023).

The operationalization of these legal bases is articulated with the principles of the LGPD, with emphasis on purpose, necessity, and transparency, including in the evaluation of less intrusive alternatives and in the documentation of processing processes in biometric systems (Baccarin, 2023). There is also reference to duties of transparency and the linking of processing to the purpose informed to the data subject, with the prohibition of subsequent incompatible uses, in addition to the enunciation of the data subject's rights such as confirmation of processing, access, correction and requests related to anonymization, blocking or deletion as the case may be (Brasil, 2018).

The LGPD provides for information security duties throughout the processing cycle, including after the end, and admits the requirement of an impact report on the protection of personal data, including sensitive, with a description of the data collected, methodology, and risk mitigation measures. This point appears as a governance parameter for operations that depend on biometric bases and automated comparison systems, given the potential impact resulting from errors and uses incompatible with the declared purpose (ANPD, 2025).

Within the scope of the federal public administration, the aforementioned Decree 10,046/2019 establishes rules and guidelines for data sharing between agencies and entities, establishes the Citizen's Base Registry, and defines biographic and biometric attributes, with biometrics understood as measurable biological and behavioral characteristics that can be collected for automated recognition (Brasil, 2019). The decree also delimits its scope by indicating that its rules do not apply to sharing with the private sector, which maintains the LGPD as a central axis for business operations and for specific cooperation outside the arrangement.

In the Citizen's Base Registry, there is a prohibition on the use of the registry or its cross-referencing with other databases for processing aimed at mapping or exploring individual or collective behaviors without express, prior and specific consent, and without transparency of motivation and purpose.

In addition, the ANPD notes that, in addition to the provisions of arts. 5 and 11 of the LGPD, can address biometrics by guiding documents and by regulation, with guidelines on concepts, legitimate contexts, legal hypotheses, observance of principles and protection measures adopted by processing agents (ANPD, 2025). Also, even when the processing occurs under legal exceptions associated with public security, national defense or criminal prosecution, data protection principles and rights must be observed.

2.2 THE PROMINENT USES OF BIOMETRIC DATA AND SYSTEMS IN BRAZIL

Biometrics, in the context of information technologies, aims to identify and map individuals, justified by security in access to goods and services and internal and border public security, in conjunction with the expansion of bases and uses in the public and private sectors (Corrêa and Loureiro, 2023).

In Brazil, for example, there is an institutional record of expansion of the processing of biometric data. This set of uses is related to state infrastructures for biometric identification and verification (ANPD, 2025), mainly in the areas of public security and criminal prosecution.

It should be noted that the constitution of biometric banks by public agencies stems from normative requirements associated with the issuance of identity documents, passports, access to public service platforms and the issuance or renewal of voter registration, situations in which the identification of the applicant includes the collection of biometric data. This data, especially fingerprints, remains stored after the service is delivered, with the possibility of later verification according to the context of collection, which characterizes the formation of civil biometric banks in the public sector (Lima et al., 2022).

Thus, it is worth mentioning, for example, the signing of cooperation agreements to allow access, by judicial police bodies, to civil biometric databases as a standard for criminal identification processes, in a scenario in which the lack of specific legislation on the production of expert evidence based on biometric standards of civil origin is pointed out (Lima et al., 2022)

In this infrastructure, the Automated Fingerprint Identification System, known as AFIS, uses fingerprints to identify individuals and seeks to prevent duplication of identification or multiple identifications assigned to the same person. The Federal Police's Manual for the Identification of Disaster Victims even recommends the use of the system and indicates, as an initial measure for obtaining ante-mortem data, the insertion of decadactylar forms for automated confrontations with questioned papilloscopic material (Federal Police, 2011 apud Souza et al., 2023).

There is also the adoption of multimodal systems, such as the Automated Biometric Identification System, known as ABIS, which admits facial recognition, palm prints, and fingerprints, with the presentation of classification by score as a measure of the level of coincidence between the sample and stored patterns (Souza et al., 2023). The Secretariat of Social Defense of Pernambuco acquired the system in 2019, and the database has been fed by new issuances of identity cards and the gradual digitization of physical medical records (BGSDS, 2019 apud Souza et al., 2023).

More recently, the Smart Sampa Program, an initiative under the responsibility of the Municipal Secretariat of Urban Security of São Paulo, is expected to install 20 thousand cameras in the city, guided by territorial criteria associated with crime rates, and with the use of algorithms that generate alerts for intrusion, vandalism and theft, in addition to identification of license plates of stolen or stolen vehicles and facial recognition aimed at locating missing persons and fugitives from the justice (São Paulo City Hall, 2025).

In the program's institutional transparency report, facial recognition appears associated with the identification of wanted and fugitives from justice and the location of missing persons, indicating that the program does not structure its own database and does not store personal data, except for images linked to an identifier referring to wanted, fugitive or missing, and with a description that access to information contained in the BNMP occurs when there is facial compatibility greater than 90 percent.

In the private sector, biometrics appears mainly as an authentication and identification technique in everyday activities, with partial displacement from traditional methods such as passwords and cards to credentials based on the holder's biological characteristics (Canuto, 2022). This movement is also associated with the logic of security in access to goods and services in the market and the diffusion of biometric identification technologies in connection with information technologies (Correa and Loureiro, 2023).

According to Canuto (2022), the biometric data used by companies can derive from various modalities, such as signature, fingerprints, and face, as well as iris, retina, voice, hand geometry, and other techniques, which expands the debate beyond facial recognition. In terms of applications, there is mention of scenarios such as logical and physical access control and fraud detection, with the use of characteristics such as face, fingerprint and voice, among others.

In the private sector, the centrality of biometric databases also intensifies discussions about the security and legality of their use, as the compromise of this data is associated with the irrevocability of the holder's characteristics, which differentiates the scenario from incidents involving passwords and justifies the adoption of specific protection techniques, such as cancelable biometrics and encryption.

2.3 CONTROVERSIES AND RISKS ASSOCIATED WITH THE USE OF BIOMETRICS

There is no unanimity regarding the public interest in the use of these systems, both in the public and private spheres. For example, the Take My Face Out of Your Sights Campaign mobilizes civil society in Brazil to press for a total ban on digital facial recognition in public security, through direct dialogue with security forces and parliamentarians, dissemination of open letters, and public education actions on the harms associated with facial recognition, with mention of the risk of perpetuating racism (EPIC, 2024).

Likewise, there are records of movements by civil organizations that demand regulation of facial recognition and, in some cases, defend a partial or complete ban, with an indication of support from entities such as LAPIN, Article 19, Data Privacy Brasil, InternetLab, and Idec for the Take My Face Out of Your Sights campaign (Baccarin, 2023).

In the public justification of these initiatives, examples associated with false alerts and approaches derived from facial recognition systems, with the allegation of selective incidence on black people, are presented. Among the cases cited, there is an episode from April 2025 in which an 80-year-old man was mistaken for a person wanted by the Justice and remained detained for 10 hours after an alert attributed to Smart Sampa cameras in a basic health unit, in addition to reports of a woman in Sergipe confused twice in 2024 and a public servant approached and taken to the police station in Rio de Janeiro due to an error of the system (Coalition Rights on the Network, 2025).

At the same time, the recent case involving Havan S.A., a retail chain, illustrates the associated risks. In 2024, the company started to publish, on social networks, videos under the name "samples of the month", with the exposure of images of people identified as perpetrators of thefts in stores, accompanied by a business justification of inhibition of the practice through public exposure (Gercina, 2024).

The monitoring system used artificial intelligence which, according to a public statement attributed to the company's management, allows identifying people when entering or leaving the store and relating the facial record to the moment of theft, which indicates the use of automated identification techniques from images captured in the establishment.

In May 2025, the ANPD received a notification from the Public Prosecutor's Office of the State of Santa Catarina with a request for an analysis of the compatibility of the practice with the LGPD, a fact that included the conduct in the authority's inspection procedure. After a preliminary analysis, the General Coordination of Inspection determined, at the end of June 2025, a preventive measure to temporarily suspend the dissemination of videos on social networks during the investigation, with an express indication of grounds in the LGPD, especially articles 6, 7, 11, 14 and 55-J, and with the identification of risk associated with the possible exposure of images of children and adolescents without precautions required by law (ANPD, 2025).

In view of this scenario, which is certainly repeated with its own particularities in other countries, it is necessary to build a specific normative framework to deal with the processing of biometric data by Artificial Intelligence.

3 AI ACT AND THE USE OF BIOMETRICS

Regulation (EU) 2024/1689 arises in a context in which AI systems circulate between Member States and can be deployed in various sectors, with the risk of regulatory fragmentation when national standards diverge and reduce the legal certainty of economic agents that develop, import or use these systems (European Parliament and Council, 2024).

Within this framework, the regulation links its justification to improving the functioning of the internal market, through a uniform legal framework for the development, placing on the market, putting into service and use of AI systems in the Union, preserving the free movement of AI-based goods and services and preventing national restrictions not provided for in the act itself.

As for its purpose, the preamble spells out the promotion of human-centred adoption of AI that is compatible with Union values, while providing for the protection of health, safety and fundamental rights provided for in the Charter, including democracy, the rule of law and environmental protection, as well as measures to support innovation.

Article 1 establishes a set of normative axes that includes harmonised rules for the placing on the market, entry into service and use of AI systems, prohibitions on certain practices, specific requirements and obligations for high-risk systems and their operators, transparency rules for certain systems, discipline for general-purpose AI models, in addition to rules for monitoring, inspection, governance and measures to support innovation with a focus on small and medium-sized companies and startups.

The regulation is intended for a chain of agents. Article 2 includes providers[3] who place on the market or put into service AI systems and providers of general-purpose AI models,

[3] In Regulation (EU) 2024/1689, an ombudsman is a natural or legal person, public authority, agency or other body that develops a general-purpose AI-system or AI-model, or that has that system or model developed and places it on the market or puts it into service under its own name or brand, with or without payment (European Parliament and Council, 2024).

even when established outside the Union, as well as deployers established in the Union, importers and distributors, manufacturers who place an AI system on the market under their name or brand, authorized representatives of providers not established in the Union, and affected persons located in the Union, when the exit from the system is used in European territory. The text excludes from its scope areas beyond the reach of Union law and declares that it does not affect competences of the Member States in matters of national security, in addition to excluding its application to AI systems used exclusively for military, defense or national security purposes.

The regulatory architecture operates by risk classification and proportional obligations, with reference in the literature to four categories, prohibited, high risk, limited risk, and minimal risk, which organizes the incidence of prohibitions, requirements, and duties throughout the life cycle of systems and models (Arantes Júnior, 2025). This structure coexists with the rule that the regulation acts in a complementary way to other branches of Union law, including data protection, consumer protection, fundamental rights, employment, and product safety, without excluding rights and means of protection provided for in these regimes.

Regulation (EU) 2024/1689 adopts definitions of biometrics in line with the vocabulary of Regulation (EU) 2016/679, by treating biometric data as personal data resulting from specific technical processing relating to physical, physiological or behavioural characteristics of the natural person, such as facial images and dactyloscopic data (European Parliament and Council, 2024). In the General Protection Data Regulation (GPDR), this notion includes the requirement to allow or confirm the unique identification of the person, also with mention of facial images and dactyloscopic data (European Parliament and Council, 2016).

This conceptual coordination is important because the GDPR classifies as a special category the processing of biometric data for the purposes of unique identification and establishes, as a rule, the prohibition of such processing, except in the cases provided for in Article 9 itself. The AI Act incorporates this logic by establishing that, outside the specific scope of use for criminal prosecution purposes in publicly accessible spaces, biometric processing remains subject to the requirements of the GDPR, and for non-public safety purposes, Article 9 of the GDPR operates as a prohibition rule with limited exceptions.

The AI Act operates through a risk-based regulatory dynamic, with differentiation of obligations according to the category of the system, a logic also described in the literature as a structure that segments prohibited, high-risk, and minimal- or low-risk systems (Monteiro, 2026).

Thus, when it comes to biometrics, the regulation defines operational categories to delimit obligations and prohibitions. Biometric *identification* refers to automated recognition to establish identity by comparison with a reference base, while biometric *verification* designates one-to-one verification, including authentication.

The text also differentiates *remote biometric identification*, which identifies people without active participation, typically at a distance, by comparison with the reference base, and explains the *real-time* modality when capture, comparison and identification occur instantaneously, or almost.

Emotion recognition system is defined as a system that infers emotions or intentions from biometric data, and *biometric categorisation system* as a system that assigns categories based on biometrics, except for the hypothesis of an accessory function and necessary for objective technical reasons.

Article 5 of the AI Act lists prohibited practices, with a direct impact on biometrics. These include the creation or expansion of facial recognition bases by non-targeted scraping of facial images on the internet or in CCTV.[4]

The regulation also prohibits categorization systems that, based on biometric data, deduce or infer race, political opinions, union membership, religious or philosophical beliefs, sex life, or sexual orientation, with delimited caveats for labeling or filtering of lawfully acquired biometric data sets and for categorizations in the context of public security.

As for the use of real-time remote biometric identification in publicly accessible spaces for public safety purposes, the AI Act establishes a prohibition with typified and conditioned exceptions. That is, the text admits the use only when strictly necessary for the targeted search of specific victims and missing persons, prevention of substantial and imminent threat to life or physical safety or terrorist threat, or location and identification of suspects for serious crimes defined by reference to the annex and maximum penalty threshold.

For the implementation of these exceptions, the regulation provides for safeguards, with the requirement of an impact assessment on fundamental rights and registration of the system, with an exception admitted for urgency for registration, without ruling out its subsequent conclusion.

The AI Act associates biometrics with high-risk cases, with normative justification linked to discriminatory effects and biases, especially in remote biometric identification, which is why it should be treated according to this particularity. For high-risk systems, the regulation

[4] CCTV is the acronym for *closed circuit television*, in Portuguese "closed circuit television". It refers to camera systems that capture and transmit images to a restricted set of monitors, recorders, or monitoring centers, rather than transmitting publicly. In urban and private contexts, CCTV usually designates video surveillance networks used for security, access control and occurrence registration.

imposes a risk management system throughout the life cycle, defined as a continuous and iterative process with identification of known and foreseeable risks, assessment of risks under normal use and foreseeable misuse, and adoption of targeted mitigation measures.

The text also establishes a duty of testing to identify risk management measures, with execution before placing on the market or putting into service, with probabilistic metrics and thresholds compatible with the intended purpose.

In the data dimension, it is required that training, validation and testing sets be subjected to governance and management practices appropriate to the purpose, covering data origin and original purpose, preparation operations such as labeling and cleaning, formulation of assumptions, and examination of biases with the potential to affect fundamental rights or lead to discrimination prohibited in Union law, with measures to detect, prevent and mitigate.

Similarly, at the organizational level, the regulation requires providers of high-risk systems to maintain a quality management system with documented policies and procedures, including compliance strategies, testing and validation procedures, and data management systems.

These requirements are directly related to the impact on fundamental rights. For this reason, it also provides for the assessment of these impacts prior to the use of the biometric system, and must contain a description of the process in which the system will be used, period and frequency of use, potentially affected categories, risks of damage and human supervision measures, among other elements. This obligation is an ex ante requirement for high-risk systems in the European Union, with the possibility of updating when information becomes obsolete (Monteiro, 2026).

4 ANALYSIS OF PL 2338/2023 FROM THE PERSPECTIVE OF THE USE OF BIOMETRICS

The current normative discussion on artificial intelligence in Brazil takes place in a scenario in which there are already rules that touch on automated systems, such as the General Data Protection Law and the Digital Government Law, without there being, so far, a specific and comprehensive normative framework aimed exclusively at the regulation of AI. In this context, the topic became part of the legislative agenda under the argument of the need to keep up with technological advances and to face risks related to privacy, security, transparency, and the protection of fundamental rights, with the convergence of the debate in PL 2,338/2023 (Arantes Júnior, 2025).

The project is presented as a proposal for a legal framework to regulate the use, implementation, and development of AI systems in the country, with mechanisms associated with impact assessments and governance structures articulated with the protection of personal data (Monteiro, 2026).

In the same sense, the project adopts a logic of regulation by risk, with the definition of categories and the imposition of denser obligations for systems classified as high risk, including impact assessment provisions, transparency mechanisms, and the possibility of auditing and supervision by competent authorities (Arantes Júnior, 2025).

The processing of PL 2,338/2023 is connected to previous initiatives that sought to discipline the use of AI systems in Brazil, with emphasis on PL 21/2020, which proposed principles, rights, and duties, and which was declared impaired in December 2024 due to the subsequent processing of more comprehensive proposals in the Senate. In addition, other related projects were joined or considered impaired, under the justification of avoiding regulatory overlap and concentrating the debate around a single regulatory framework.

In this context, PL 2.338/2023, authored by Senator Rodrigo Pacheco, was approved by the Federal Senate and sent to the Chamber of Deputies in March 2025. PL 2,338/2023 organizes obligations based on a risk classification model and provides that systems considered to be high risk, after preliminary assessment, are subject to algorithmic impact assessment, defined as a continuous iterative process throughout the life cycle, with periodic updates whose periodicity depends on regulation by the competent authority, in addition to being expected to be carried out by professionals with functional independence and technical knowledge, scientific and legal aspects.

In the doctrinal characterization, this engineering seeks to anticipate potential damages associated with the operation of the systems, with a record of known and foreseeable risks and adverse consequences, in parallel with mechanisms aimed at transparency and accountability (Monteiro, 2026).

4.1 ORGANIZATION OF THE BILL AND PROVISIONS ON BIOMETRICS

The text approved in the Chamber introduces operational definitions to differentiate biometric identification and biometric authentication. Biometric identification appears as a method that involves the recognition of human physical, physiological, and behavioral characteristics for the purpose of identifying an individual, while biometric authentication is associated with the process of verifying or confirming identity by comparing biometric characteristics with a previously stored model (Brasil, 2023). Thus, it creates a conceptual basis to separate uses aimed at attributing identity to an open set of people, in the case of identification, from uses aimed at confirming a previously declared identity, in the case of authentication.

In the risk classification regime, the Bill provides for specific prohibitions related to biometrics in spaces accessible to the public. Article 13, item IV, prohibits the development, implementation, and use of real-time remote biometric identification systems in spaces accessible to the public, admitting exceptions linked to delimited hypotheses, such as investigation instruction or criminal proceedings upon prior and motivated judicial authorization and other contexts listed in the provision (Brasil, 2023).

In addition to the prohibitions, the Bill classifies certain biometric uses as high risk. Among the hypotheses listed, there is the use of biometric identification and authentication systems for the recognition of emotions, with the exception of biometric authentication systems whose sole purpose is the confirmation of a specific natural person. This normative option delimits a cut in which the risk does not arise only from the use of biometrics, but from the inferential objective associated with the system, in this case, inferences about affective states (Brasil, 2023).

In the scope of governance and procedural obligations, the Bill deals directly with biometric systems for identification purposes in the public sector. Article 23, paragraph 1, establishes that the use of biometric systems for identification purposes must comply with the principles and governance measures of the law and must be preceded by an algorithmic impact assessment, with observance of guarantees for the exercise of the rights of affected people or groups and protection against direct, indirect, illegal or abusive discrimination.

Thus, paragraph 2 provides that, if there is no substantive elimination or mitigation of the identified risks, the use will be discontinued

In the Chamber of Deputies, a controversy arises around facial recognition technologies in public spaces, especially when associated with public security and criminal prosecution. A document from civil society organizations registers opposition to the proposal attributed to rapporteur Aguinaldo Ribeiro to loosen rules on the use of facial recognition in public spaces and mentions a statement in which the text approved by the senators was described as too restrictive (Coalition Rights on the Network, 2025).

In the same document, it is pointed out that the wording of the Bill classifies facial recognition technologies as of excessive risk, but with a broad list of exceptions that encompasses current uses in the context of public security and criminal prosecution, with reference to article 13, item VII, and with criticism of a scenario in which exceptions would be outside the proposed governance structure

4.2 CONVERGENCES AND NEW PERSPECTIVES BETWEEN PL 2338/2023 AND THE EUROPEAN UNION'S AI ACT

Both normative texts adopt a logic of escalation by risk, with a set of prohibitions for uses considered incompatible with rights and freedoms and a regime of reinforced obligations for uses classified as high risk. In the AI Act, article 5 brings together prohibited practices, including for reasons associated with surveillance and impacts on fundamental rights, and establishes delimited exceptions for remote biometric identification in real time in publicly accessible spaces for law enforcement purposes, linked to specific objectives and a cut of crimes referred to in the annex (European Union, 2024).

In PL 2338/2023, article 13 prohibits, as a rule, the use of biometric identification systems at a distance in real time in spaces accessible to the public, with exceptions associated with criminal investigation and prosecution, search for victims and missing persons, serious and imminent threat, flagrante delicto, and compliance with warrants, under requirements such as prior judicial authorization and judicial control when applicable (Brasil, 2023).

There is also convergence in the provision of governance measures and documentation for high-risk uses. The Bill requires, in the public sector, access and use protocols with registration of who used the system, the right to human explanation and review, and publication of preliminary assessments, in addition to imposing algorithmic impact assessment for the use of biometrics for the purpose of identification and discontinuity of use when there is no substantive elimination or mitigation of risks.

In the AI Act, the high-risk discipline connects to evaluation, registration and supervision mechanisms, including requirements that relate registration on a European basis and synthesis of impact assessment on fundamental rights in certain registration and reporting contexts.

Finally, in this context, the main comparative implication for Brazil, with an exclusive focus on biometrics, lies less in the reaffirmation of the core already provided for in article 13, item IV, and more in the possibility of expanding the discipline to other biometric uses with potential for identification and surveillance.

5 FINAL CONSIDERATIONS

As seen, Bill No. 2338/2023 already incorporates direct discipline for biometric identification at a distance in real time in spaces accessible to the public, by prohibiting the development, implementation, and use of this practice, with delimited exceptions, such as instruction of an investigation or criminal proceeding upon prior and motivated judicial authorization, search for victims and missing persons, serious and imminent threat, flagrante delicto, and recapture and compliance with warrants, in addition to requiring proportionality and strict necessity, judicial control, and review of algorithmic inference by a public agent, with reference to the principles and rights of the law itself and, where applicable, of the LGPD (Brasil, 2023).

The AI Act structures a similar solution by treating real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement activities, with a regime that starts from prohibition and admits use only when strictly necessary for exhaustive purposes, such as targeted search for specific victims and missing persons, prevention of specific threat, substantial and imminent to life or physical safety or terrorist threat, and locating or identifying a suspect for investigation, prosecution or criminal prosecution of offences referred to in the Annex and punishable by a maximum sentence of at least four years, with a requirement that the use confirm the identity of the individual specifically targeted (European Union, 2024)

Thus, from these perspectives, it is understood that a conceptual evolution is possible by incorporating operational definitions that the AI Act presents for biometric data, biometric identification, biometric verification, remote biometric identification system, real-time remote biometric identification, and subsequent remote biometric identification, including the element of absence of active involvement of the holder and the criterion of significant delay in distinguishing between real-time and later.

Still on remote biometric identification, the AI Act explains institutional safeguards that can guide Brazilian design for uses admitted in exception, such as the requirement of an impact assessment on fundamental rights, registration of the system on its own basis, prior authorization by an independent judicial or administrative authority with a binding decision, the possibility of starting without authorization only in urgency with a request within 24 hours, and the duty to interrupt use and discard and eliminate data and results when authorization is denied, in addition to prohibiting decisions with adverse legal effect based exclusively on leaving the system.

The Bill, in turn, provides that the use of biometric systems for identification purposes observes governance principles and measures and is preceded by algorithmic impact assessment, with guarantees for the exercise of rights and protection against discrimination, and determines discontinuity of use when there is no substantive elimination or mitigation of risks, in addition to establishing protocols for access and registration of use in the public sector, the right to human explanation and review and the publication of preliminary assessments.

In this comparison, one possibility of improvement guided by the AI Act consists of detailing, for remote biometric uses in exception, procedural and supervisory obligations external to the user entity, with systematic registration and audit trail, authorization criteria, and duties of disposal and elimination associated with the denial or termination of the measure.

The AI Act also brings a prohibition that does not appear in an equivalent way in the Bill when prohibiting systems that create or expand facial recognition bases by non-targeted collection of facial images on the internet or in CCTV images, which closes the door to the formation of biometric banks from massive extraction without a defined target. Based on this parameter, the Bill may incorporate a specific clause to prevent the creation and expansion of facial biometric databases by non-targeted scraping, with wording that covers both open sources and video surveillance images, in a manner compatible with the LGPD and the sensitive data protection regime.

Another difference focuses on emotion recognition systems. The Bill classifies as high risk biometric identification and authentication systems intended for the recognition of emotions, except for authentication whose sole purpose is the confirmation of a specific natural person, which triggers general obligations of the high-risk and governance regime. The AI Act, on the other hand, prohibits systems intended to infer emotions in the workplace and educational institutions, except when the use is intended for medical or security reasons, and also defines an emotion recognition system as one that identifies or infers emotions or intentions based on biometric data.

Based on this, the elaboration of the Bill can consider a contextual prohibition for the recognition of emotions at work and education, or, if it maintains the option for high risk, it can delimit strict hypotheses and specific purposes, with additional requirements of justification, human supervision and transparency to the affected due to the asymmetry in these environments.

There is also a biometric vector that the AI Act expressly treats and that the Bill does not yet describe with equal density, the biometric categorization. The AI Act prohibits biometric categorization systems that, based on biometric data, deduce or infer race, political opinions, union membership, religious or philosophical beliefs, sex life, or sexual orientation, while defining biometric categorization system as one that assigns natural persons to specific categories based on their biometric data, with the exception of ancillary and technically necessary cases.

This parameter offers Brazil an additional path, with a prohibition rule directed to sensitive inferences from biometrics, which will serve to reduce ambiguities when biometric systems do not intend to identify by name, but operate by classification and inference, including in private and service environments.

The distinction between real-time and post-time remote biometric identification also yields comparative implications. The literature that examines the European proposal pointed out questions about the separation between real and later time and about the line between biometric categorization and biometric identification, indicating that the distinction can generate classificatory arbitrariness (Madiega; Mildebrath, 2021 apud Baccarin, 2023).

The AI Act, in addition to defining the subsequent system as the remote one that is not in real time, registers the need for safeguards for subsequent uses and removes the possibility of indiscriminate surveillance and circumventing the strict conditions of real time, by requiring targeted use in terms of individuals, location and time frame, based on a closed set of legally obtained images.

Along these lines, the Bill can explain how it treats subsequent remote biometric identification, either by extending the discipline of article 13 beyond real time, or by its own chapter of safeguards that covers ex post uses in video surveillance and other bases, focusing on the prevention of generalized scans and the delimitation of scope and reference base.

Finally, the AI Act offers a biometric perspective of institutional arrangement of transparency and accountability that can be adapted to Brazil. In the use of real-time remote biometric identification for law enforcement purposes, the regulation provides for notification to supervisory authorities and aggregated annual reports, with publication by the Commission of annual reports on use, without sensitive operational data.

In the Bill, there is provision for the publication of preliminary assessments of high-risk systems in the public sector and the establishment of minimum standards of transparency at the federal level, in addition to protocols for access and registration of use and the right to human explanation and review.

Based on this contrast, it is possible to combine the Brazilian model of administrative evaluation and transparency with a national registry of remote biometric uses and with periodic aggregate reporting obligations, which expands public traceability without exposing sensitive operational information, especially in contexts of security and border control.

REFERENCES

Brasil. Autoridade Nacional de Proteção de Dados. (2023, 6 de julho). Análise preliminar do Projeto de Lei (PL) nº 2338/2023. https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf

Brasil. Senado Federal. (2023). Projeto de Lei n.º 2.338, de 2023. Dispõe sobre o uso da inteligência artificial. https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

Canuto, A. M. de P. (2022). Ética no uso de dados biométricos: Histeria ou uma preocupação coerente? Computação Brasil, 47, 36–39. https://doi.org/10.5753/compbr.2022.47.4406

Coalizão Direitos na Rede. (2025, 8 de dezembro). Posicionamento sobre o PL 2338/2020 e sistemas de identificação biométrica (reconhecimento facial). https://direitosnarede.org.br/2025/12/08/posicionamento-pl-2338-sistemas-identificacao-biometrica-reconhecimento-facial/

Corrêa, A. E., & Loureiro, M. F. B. (2023). Biometria, autodeterminação informativa e proteção de dados pessoais. Revista de Direito Civil Contemporâneo, 36, 47–74.

Electronic Privacy Information Center. (2024, 29 de maio). EPIC awards the Tire Meu Rosto da Sua Mira campaign as EPIC International Privacy Champions. https://epic.org/epic-awards-the-tire-meu-rosto-da-sua-mira-campaign-as-epic-international-privacy-champions/

Gercina, C. (2024, 15 de outubro). Havan expõe em vídeos “amostradinho do mês” supostos furtos nas lojas. Folha de S.Paulo. https://www1.folha.uol.com.br/mercado/2024/10/havan-expoe-em-videos-amostradinho-do-mes-supostos-furtos-nas-lojas.shtml

Lima, N. A., et al. (2024). O uso de bancos de dados biométricos civis em investigações criminais: Possíveis avanços à luz de direitos e garantias fundamentais. Revista Jurídica da Seção Judiciária de Alagoas, 1(8), 135–152. https://revista.jfal.jus.br/RJSJAL/article/view/56

São Paulo (Município). Secretaria Municipal de Segurança Urbana. (2024, 3 de julho). Programa Smart Sampa. https://prefeitura.sp.gov.br/web/seguranca_urbana/w/smart-sampa-2

Schwertner, S. D. G. (2025, 6 de novembro). Projeto de lei impõe mais limites à utilização de dados biométricos. Consultor Jurídico. https://www.conjur.com.br/2025-nov-06/o-uso-indiscriminado-de-dados-biometricos-e-o-pl-2-379-2025/

Souza, I. D. D., Silva, D. R. da C., Almeida, A. C. de, & Andrade, E. S. de S. (2023). Aplicação do ABIS na identificação de vítimas de desastres: Utilização dos bancos de dados biométricos. Revista de Estudos Interdisciplinares, 5(6), 227–244. https://doi.org/10.56579/rei.v5i6.793

União Europeia. (2016). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

União Europeia. (2024). Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. Relativo à criação de regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial). https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689

Violato, R. P. V., Neto, M. U., Simões, F. O., Pereira, T. de F., & Angeloni, M. de A. (2013). BioCPqD: Uma base de dados biométricos com amostras de face e voz de indivíduos brasileiros. Cadernos CPqD Tecnologia, 9(2), 7–18.