LEXOLOGY

Digital Law in Brazil - Current Hot Topics | Facial Biometrics and the LGPD: Advances, Risks and Regulatory Trends

Montaury Pimenta, Machado & Vieira de Mello

Brazil | February 11 2026

The use of facial biometrics has become one of the most widespread technologies driving digital transformation in recent years. From authentication systems on mobile devices to access control in companies and residences, biometric identification has become common practice in various settings. This accelerated growth, however, brings significant legal challenges, especially regarding the protection of personal data under the Brazilian General Data Protection Law ("LGPD") - Law No. 13.709/2018.

These challenges arise mainly because biometric data are classified by the LGPD as sensitive personal data, given that they relate to characteristics capable of uniquely identifying a natural person. As a result, a higher level of protection and caution is required. In practical terms, if such data are exposed or improperly captured, the risk extends to any system that relies on the same biometric trait for authentication, potentially causing permanent harm. Moreover, facial recognition systems may amplify additional risks such as algorithmic discrimination, excessive surveillance, and behavioral profiling, with material impacts on decisions that affect data subjects' rights.

In this context, it is important to emphasize that the LGPD requires the processing of biometric data to be grounded in a specific and robust legal basis, significantly restricting available alternatives for those intending to process this type of sensitive personal data. As a rule, the most relevant bases include: (i) explicit consent, provided it is freely given, informed, and unequivocal — the most common basis, though not always appropriate where there is an imbalance in the relationship (such as employer and employee); (ii) fraud prevention and data subject security, applicable in exceptional situations; and (iii) compliance with legal or regulatory obligations, particularly relevant in sectors such as finance and air transportation.

Beyond identifying an appropriate legal basis, the processing of biometric data must also adhere to the LGPD's core principles, including: (i) purpose limitation, requiring specific, legitimate, and explicit purposes, and prohibiting further processing for incompatible objectives; (ii) data minimization, restricting collection to what is strictly necessary; (iii) transparency, ensuring that data subjects receive clear, precise, and easily accessible information; and (iv) security, through adoption of technical and administrative measures capable of protecting data against unauthorized access, loss, or alteration.

Accordingly, data controllers must always demonstrate the strict necessity of collecting biometric information, assessing whether less intrusive solutions could achieve the same objective, such as temporary passwords, QR codes, or physical access cards. Independent audits and data protection impact assessments are also recommended, as well as the implementation of clear retention and deletion policies and effective channels for the exercise of data subject rights.

Given the relevance of the topic, the Brazilian Data Protection Authority ("ANPD") — the regulatory agency responsible for enforcing and overseeing compliance with the LGPD — has already signaled concern regarding the large-scale use of facial biometrics. In a recent public consultation, the ANPD launched a "Call for Contributions" aimed at gathering input from society to guide its future regulatory and advisory actions on

biometric data processing. In this scenario, specific regulation is expected, providing clear guidelines on proportionality, appropriate legal bases, prevention of discriminatory impacts, and the promotion of transparency and accountability in the use of biometric data by both public and private actors.

The international regulatory debate — including the European AI Act and growing restrictions on the use of facial recognition by public authorities in various jurisdictions — is also noteworthy and is likely to influence the evolution of the Brazilian regulatory framework.

Companies that already use or plan to use facial biometrics should therefore adopt a preventive and strategic approach. Best practices include reassessing the necessity of the technology to avoid disproportionate or merely convenient uses; strengthening explicit consent with accessible language and easy revocation mechanisms; implementing strong security controls, with particular attention to preventing security incidents; defining clear retention and disposal policies, ensuring data are deleted once the purpose has been fulfilled; training staff to mitigate operational risks; and fostering a culture of privacy.

In conclusion, facial biometrics will remain a central topic in Digital Law, both due to its innovative potential and the considerable risks it may pose. For organizations, understanding the LGPD's requirements and aligning internal practices with modern governance and security standards are essential not only to avoid sanctions but also to maintain data subject trust and build ethical and sustainable technological solutions.

Montaury Pimenta, Machado & Vieira de Mello - Júlia Bessa Sanzi