DIGITAL LAW

DIGITAL NEWSLETTER

17TH EDITION

Check out the latest news in this edition

ALMEIDA ADVOGADOS
CORPORATE LAW

25 ANOS | YEARS

ALMEIDA ADVOGADOS
CORPORATE LAW
25 ANOS | YEARS

DIGITAL NEWSLETTER

17TH EDITION

This is the newsletter created by our Digital Law Team, aiming to gather the most relevant news and discussions on topics from the digital world. Enjoy your reading!

BRAZIL AND THE EUROPEAN UNION RECOGNIZE MUTUAL ADEQUACY IN PERSONAL DATA PROTECTION

On the eve of International Data Protection Day, Brazil and the European Union have mutually recognized the adequacy of their personal data protection regimes, enabling cross-border data transfers between the two jurisdictions without the need for additional safeguards. The recognition is based on the equivalence between Brazil's General Data Protection Law (LGPD) and the EU's General Data Protection Regulation (GDPR), including the existence of independent supervisory authorities and effective enforcement mechanisms.

The decision provides greater legal certainty for companies and public bodies, reduces compliance costs for international data transfers, and strengthens regulatory cooperation —particularly between the Brazilian National Data Protection Agency (ANPD) and EU data protection authorities—placing Brazil among jurisdictions deemed adequate by the European Union.

CYBERCRIME EVOLVES INTO AN INDUSTRIAL-SCALE OPERATION DRIVEN BY ARTIFICIAL INTELLIGENCE

Fortinet report Cyber Threats Previsions for 2026 indicates that cybercrime has begun operating on an industrial scale, driven by the strategic use of artificial intelligence to automate attacks, reduce costs, and increase fraud success rates. AI-based tools enable large-scale, highly personalized phishing campaigns, increasingly realistic deepfakes, automated vulnerability exploitation, and real-time attack adaptation, significantly raising threat sophistication.

This evolution lowers technical barriers to entry and expands attack reach, allowing criminal groups to function as structured organizations with role specialization, crime-as-a-service models, and transnational operations. The landscape heightens operational, financial, and reputational risks for companies and governments, demanding equally sophisticated responses grounded in threat intelligence and coordinated defense strategies.

ANPD EXTENDS DEADLINE FOR COMPANIES TO SUBMIT INFORMATION ON THE IMPLEMENTATION OF THE DIGITAL ECA RULES

Brazil's National Data Protection Agency (ANPD) has extended the deadline to February 13, 2026, for companies to submit information on the measures adopted to comply with the new rules under the so-called Digital ECA (Brazil's digital child and adolescent protection framework). The extension was granted in the context of a monitoring action and aims to allow more consistent and complete responses, given the complexity of the requirements and the year-end period.

The initiative involves 37 tech companies with significant reach among children and adolescents and has an informational and diagnostic nature, with no sanctioning intent at this stage. The objective is to assess market compliance levels and identify practical implementation challenges, supporting future guidance and enforcement actions by the ANPD.

PORNHUB TARGETED IN EXTORTION ATTEMPT AFTER HACKERS STEAL PREMIUM USER ACTIVITY DATA

Adult content portal Pornhub was targeted in an extortion attempt after hackers claimed to have gained access to sensitive data related to the activity of premium users on the platform. The information reportedly includes usage logs and content consumption patterns, whose exposure could severely compromise subscribers' privacy.

The attackers demanded payment in exchange for not disclosing the data, in a typical data extortion scheme without system encryption. The company stated that it launched an internal investigation and confirmed that no financial data was compromised, highlighting the significant privacy and reputational risks associated with data leaks involving adult content platforms.

ONLY 27% OF BRAZILIAN COMPANIES HAVE FORMAL RULES GOVERNING THE USE OF ARTIFICIAL INTELLIGENCE

While AI adoption is accelerating in the Brazilian corporate environment, most companies still operate without clear internal guidelines. According to data from the Third Edition of the Sectoral Survey on Digital Risk Maturity of Brazilian Companies, only 27% of organizations have formal policies defining limits, responsibilities, and criteria for AI use, reflecting low maturity in technological governance and risk control.

The lack of rules increases exposure to operational, legal, and reputational risks, particularly in activities involving automated decision-making, personal data processing, and generative AI tools.

GROK CASE REIGNITES DEBATE ON THE LIMITS OF AI FOLLOWING ALLEGATIONS OF MISUSE

Following allegations that Grok was used to create non-consensual sexually explicit deepfake images, the debate over the risks and limits of artificial intelligence intensified. The episode illustrates how generative AI tools can be exploited for abusive practices, amplifying harm to privacy, dignity, and reputation, particularly when effective safeguards against illicit or unethical uses are lacking.

The case involving the AI developed by xAI raises concerns about developer responsibility, technological governance, and the need for more robust safeguards. It exposes gaps in content moderation, deepfake prevention, and protection against digital abuse, reviving regulatory and ethical discussions about how far AI systems can be made publicly available without strict control and human oversight mechanisms.

RESEARCHERS DEMONSTRATE THE COMPROMISE OF VOICE AUTHENTICATION SYSTEMS

Researchers successfully bypassed commercially deployed voice authentication systems, showing that artificially generated or manipulated audio samples can deceive biometric verification mechanisms. Tests revealed that even solutions claiming additional safeguards —such as vocal pattern analysis and behavioral verification—failed to distinguish real voices from well-crafted synthetic audio.

The technical demonstration relied on voice cloning and synthesis models trained with only a few seconds of original audio, enabling accurate replication of victims' timbre and intonation. The findings expose concrete vulnerabilities in systems used by banks, call centers, and digital platforms, indicating that voice biometrics can be exploited as a fraud vector when used as a primary authentication factor.

HP REPORT FINDS THAT 57% OF MALWARE IN 2025 ARE INFOSTEALERS

An HP report indicates that 57% of malware samples analyzed in 2025 fall into the infostealer category, malicious code designed to steal credentials, session cookies, financial data, and corporate information. The data highlights a shift toward silent data exfiltration rather than destructive attacks or system disruption.

The report shows that infostealers are primarily distributed through phishing campaigns, trojanized software downloads, and malicious documents, often exploiting reused credentials and remote corporate access. Their prevalence is directly linked to rapid data monetization for immediate fraud or as fuel for subsequent targeted attacks and extortion.

ANPD PUBLISHES PRIORITY TOPICS MAP FOR 2026–2027 AND UPDATES REGULATORY AGENDA

Brazil's National Data Protection Agency (ANPD) published its Priority Topics Map for the 2026–2027 biennium, alongside an update to its 2025–2026 Regulatory Agenda, outlining the areas that will guide its regulatory, supervisory, and guidance activities. The document organizes topics by relevance, impact, and urgency, providing greater regulatory predictability to the market.

Key focus areas include data protection governance, processing of sensitive personal data, data subject rights, information security, international data transfers, and emerging technologies such as artificial intelligence.

AI-RELATED RISK JUMPS FROM 10TH TO 2ND PLACE IN ALLIANZ GLOBAL RISK RANKING

A global Allianz study shows that risks associated with artificial intelligence climbed from 10th to 2nd place among corporate risk concerns, second only to business interruption. The shift reflects widespread AI adoption and a growing number of incidents involving technical failures, misuse, flawed automated decisions, and sensitive data exposure.

The study links AI risks to cybersecurity, civil liability, regulatory compliance, and reputational damage. Increasing reliance on automated models for critical decisions amplifies the impact of errors, biases, and malicious manipulation.

CHINA ORDERS COMPANIES TO STOP USING U.S. AND ISRAELI CYBERSECURITY SOFTWARE

The Chinese government has instructed domestic companies to discontinue the use of cybersecurity software developed by U.S. and Israeli firms, particularly in sensitive sectors. The directive was issued directly to major corporate groups and state-owned enterprises as part of a strategy to reduce foreign technological dependence and mitigate external access risks to data and critical infrastructure.

The move is part of broader geopolitical tensions and China's push for digital sovereignty, accelerating the replacement of foreign software with domestic solutions and reshaping the global cybersecurity market.

GOVERNMENT CONFIRMS DATA BREACH AFFECTING 9 MILLION CITIZENS IN PERNAMBUCO

The Government of Pernambuco confirmed a data breach involving approximately 9 million national ID numbers (CPF) of state residents, resulting from failures in systems managed by public administration bodies. The exposed data includes basic registration information linked to CPF numbers, affecting a significant portion of the state's population.

According to official disclosures, the incident involved databases used by state agencies and was reported after unauthorized access was identified. Authorities implemented containment measures, initiated a technical investigation to identify the breach's origin, and formally notified oversight and data protection authorities.

BRAZILIAN´S CENTRAL BANK UPDATES CYBERSECURITY REGULATION

At the end of December last year, the new regulation from the Central Bank of Brazil – BACEN 5274/2025 – updated CMN Resolution 4.893/2021, which establishes the cybersecurity policy and the requirements for contracting data processing, storage, and cloud computing services to be observed by institutions authorized to operate by the Central Bank of Brazil.

The new regulation sets forth new cybersecurity requirements for all BACEN-authorized institutions that offer digital services. Compliance with these requirements by currently operating institutions must be achieved by March 1ST 2026.

EUROPEAN UNION PRESENTS A PLAN TO EXCLUDE HIGH-RISK SUPPLIERS

The European Union has presented a plan to restrict and, in certain cases, exclude suppliers classified as high-risk from critical infrastructure and strategic technology supply chains, with a special focus on telecommunications and sensitive digital services. The initiative seeks to reduce external dependencies and mitigate risks associated with national security, espionage, foreign interference, and systemic vulnerabilities in essential networks.

The plan includes technical and geopolitical criteria for risk assessment, encourages supplier diversification, and strengthens coordination among Member States in adopting mitigation measures. The strategy is part of the European effort to strengthen digital sovereignty and protect critical infrastructure, expanding the regulatory impact on global technology companies operating in the European market.

LEGISLATIVE RADAR

BILL 6724/2025

Establishes the Functional Internet Framework for Public Services, defining functional internet as connectivity that meets minimum, measurable, and auditable performance standard, such as effective speeds, latency, stability, availability, and acceptable failure rates, necessary to ensure the continuous, stable, and secure delivery of digital public services, including telemedicine, digital education, public health systems, social assistance, and citizen services.

BILL 6721/2025

Enacts the Simplified Digital Social Oversight Act, establishing a single national digital platform that allows citizens to easily report failures or disruptions in essential public services, such as water supply, electricity, sanitation, public health, transportation, and connectivity, recognizing these reports, after minimal technical validation, as official performance indicators.

BILL 6712/2025

Establishes the mandatory prior and immediate identification of automated telephone calls, including those made through artificial intelligence systems, robocalls, or equivalent technologies, requiring that, at the very beginning of the call, the recipient be clearly informed that the call is automated, the identity of the responsible legal entity, and the option to terminate the call without any charge.

BILL 6707/2025

Proposes amendments to the Consumer Protection Code to establish strict and joint civil liability of suppliers and AI system developers for damages caused by artificial intelligence systems, including those arising from autonomous, non-programmed, or unpredictable behaviors that exceed the consumer's legitimate expectation of safety

BILL 6706/2025

Proposes amendments to the General Data Protection Law (LGPD) to institute Preventive Algorithmic Audits for artificial intelligence systems used in high-impact social decisions, such as access to credit, employment, healthcare, housing, and public services, requiring public and private data controllers to submit such systems to independent external audits at least every two years or upon material model changes, as well as to submit technical reports to the National Data Protection Authority and publish an executive summary.

BILL 6704/2025

Establishes the mandatory provision of prior, clear, and prominent notice to users regarding the recording, collection, storage, or processing of voice data by call centers, digital platforms, applications, chatbots, and virtual assistants, requiring disclosure before data capture begins, in plain language, indicating the purpose of processing and the data subject rights under the LGPD; applicable to both public and private entities, with entry into force 180 days after publication.

BILL 6586/2025

Establishes rules on transparency, explainability, and access to information regarding the use of automated decision-making systems in consumer relations, ensuring consumers' rights to be informed when automated decisions produce relevant impacts, such as credit approval, pricing, account blocking, or ranking, to access clear explanations of criteria, data, and processing logic, and to request human review and contestation through a dedicated channel.

BILL 6560/2025

Proposes amendments to the Statute of the Child and Adolescent to authorize the disclosure of images and personal data of adolescents involved in violent offenses or acts involving serious threats, equivalent to heinous crimes, as well as in cases where disclosure is necessary for the identification, search, or location of missing or fugitive adolescents

AA on social media

Follow our profile for **exclusive updates** and specialized legal content on Digital Law!

Márcio Chaves
Partner

mmchaves@almeidalaw.com.br
+55 (11) 2714 6900 | 9828

Lucca Fontana
Lawyer

lgfontana@almeidalaw.com.br
+55 (11) 2714 6900

ALMEIDA ADVOGADOS
CORPORATE LAW
25 ANOS | YEARS