DIGITAL LAW

DIGITAL NEWSLETTER

15TH EDITION

Check out the latest news in this edition

ALMEIDA ADVOGADOS

ALMEIDA ADVOGADOS
CORPORATE LAW

DIGITAL NEWSLETTER

15TH 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!

INVESTOR LOSES R$ 500 MILLION IN BITCOIN AFTER SOCIAL ENGINEERING SCAM

An investor lost 783 bitcoins—around R$ 500 million—after criminals impersonated exchange and hardware wallet support, tricking him into entering his seed phrase on a malicious site. The stolen assets were quickly moved and laundered through mixers to obscure the trail. On the same day, another victim in Wales lost R$ 15.5 million in a similar scam, suggesting coordination or a growing pattern of such attacks.

RIO DE JANEIRO POLICE OPERATION TARGETS CYBER EXTORTION AGAINST LOGISTICS COMPANY

Rio de Janeiro's Civil Police launched "Operation Ghost" to counter a cyberattack targeting a logistics company. The attacker demanded US$ 10,000 in cryptocurrency in exchange for not leaking customer and supplier data. Despite the payment, internal data was leaked and the company's WhatsApp account was hacked, prompting device seizures and a criminal investigation.

PASSWORD MANAGER FLAW EXPOSES MILLIONS OF USERS

A failure in password managers exposed millions of stored credentials, putting user data at significant risk. The flaw allowed malicious actors to access sensitive information easily, highlighting the urgent need for software updates. Users are advised to enable two-factor authentication, strengthen and regularly update passwords, and ensure their password managers are patched—key steps to reduce the risk of future breaches.

BRAZIL: CYBERATTACK ATTEMPTS HIT 80% OF COMPANIES IN THE PAST YEAR

The CIO Report 2025, conducted by Logicalis with Vanson Bourne, found that 80% of large Brazilian companies faced at least one cyber incident over the past 12 months. The most common threats were malware and ransomware (40%), malicious deepfakes (37%), data breaches (34%), AI-driven attacks (31%), and phishing (28%). In 84% of cases, there was a confirmed security breach, and nearly 30% of organizations experienced multiple incidents.

ADVANCED PHISHING AND BACKDOORS TARGET CORPORATE LEADERS

A cyberespionage campaign linked to the APT MuddyWater group is targeting CFOs and financial executives across multiple regions. The attackers use highly tailored phishing disguised as Rothschild & Co recruitment emails, hosted on Firebase domains with fake CAPTCHAs to bypass suspicion.

Victims are redirected to ZIP files that deploy legitimate tools such as NetBird and OpenSSH, configured to establish persistent backdoors. The malware creates a hidden admin account, enables RDP, alters firewall rules, and schedules auto-restarts, ensuring stealthy access and enabling sensitive financial data exfiltration.

CRIMINALS USE UNCERTIFIED TV BOX DEVICES TO STEAL USER DATA, SAYS ANATEL

Brazil's telecom regulator Anatel reported that uncertified TV Box devices are being used by criminals to steal users' personal data. These devices, which provide illegal access to pay TV and streaming platforms, also serve as an entry point for malware compromising home networks.

According to the agency, only certified devices meet minimum security standards. Enforcement actions, product seizures, and consumer awareness campaigns have been announced to curb the illegal market.

HACKERS BREACH NORWEGIAN DAM, CAUSING 500 L/S WATER LEAK

Hackers compromised the Rizevatnet dam system in Norway and opened a gate for about four hours, releasing 500 liters of water per second. The attack was made possible by weak passwords in the remote control systems.

Although the incident was serious, the river's capacity absorbed the flow, preventing damage or casualties. Norwegian authorities linked the attack to a pro-Russian hacker group, but Russia's embassy denied any role.

CYBERSECURITY BUDGETS GROWTH DROPS BY HALF

Cybersecurity spending slowed sharply in 2025, with average growth of only 4%, compared to 8% in the previous year. According to IANS Research and Artico, security's share of IT budgets fell from 11.9% to 10.9%, marking the first decline in five years. While 51% of CFOs still classify cyber threats as a critical risk, budget allocations are not keeping pace with the expanding digital threat landscape.

The downturn comes even as Gartner projects global security spending to reach US$ 213 billion this year. Analysts note that regulatory pressure and growing awareness will likely sustain investments in the medium term, especially among small and midsize businesses. In the short term, however, hiring freezes, project restrictions, and tighter budgets leave organizations more vulnerable to attacks and increase the risk of major incidents.

REDUCED BUDGETS ACCELERATE AI USE IN CYBERSECURITY

With shrinking budgets and slower growth in security spending (from 17% in 2022 to 4% in 2025), organizations are increasingly turning to AI-based automation to offset staff shortages, maintain defenses, and handle rising threats. Gartner projects global information security spending at US$ 213 billion in 2025, reaching US$ 240 billion in 2026, still lagging behind demand.

Reports from IANS and Swimlane show that budget pressures, reduced government support, and global uncertainty are pushing teams to "do more with less." AI tools help with alert triage and threat detection but increase technological dependency and may introduce new risks in the medium term.

ANPD AND NIC.BR SIGN COOPERATION AGREEMENT ON DATA PROTECTION

Brazil's ANPD (National Data Protection Authority) and Nic.br (Information and Coordination Center for .BR) signed a cooperation agreement during the 16th Seminar on Privacy and Personal Data Protection in São Paulo. The initiative aims to foster joint actions in data protection and information security, including educational programs, information sharing, technical reports, and research projects.

The agreement expands on a 2021 partnership and includes the development of indicators, technical notes, and studies on privacy, cybersecurity, and artificial intelligence. According to ANPD President-Director Waldemar Gonçalves, the cooperation strengthens Brazil's data protection culture and supports regulatory harmonization, seen as key to facilitating cross-border data flows, economic cooperation, and innovation.

ANPD SUPPORTS TRANSPARENT LEGISLATION FOR EFFECTIVE AI GOVERNANCE

Waldemar Gonçalves, President-Director of the ANPD (Brazil's National Data Protection Authority), argued at a congress in São Paulo that Brazil's AI regulation should emphasize transparency, safety, explainability, protection of fundamental rights, and algorithmic non-discrimination. He affirmed the agency's readiness to coordinate the National System for AI Regulation and Governance (SIA), support Bill 2.338/2023, and lead initiatives like a regulatory sandbox and the Radar Tecnológico. International cooperation with bodies such as the Ibero-American Data Protection Network (RIPD) was also highlighted to harmonize regulations.

LUSOPHONE COUNTRIES STRUCTURE COOPERATION AND REGULATORY HARMONIZATION IN PRIVACY

At a parallel event to the 16th Privacy Seminar in São Paulo, data protection authorities from Portuguese-speaking countries formally established the Lusophone Data Protection Network (RLPD). They set up Working Groups focusing on priority areas—such as biometrics, neurodata, AI, surveillance, and cross-border data transfers—and initiated a comparative study of national laws. A network logo and website were also launched to enhance cooperation

BRAZILIAN NATIONAL DATA PROTECTION AUTHORITY (ANPD) TO GAIN AUTHORITY TO REMOVE ILLICIT DIGITAL CONTENT

The federal government plans to expand the powers of the ANPD— the Brazilian National Data and Digital Services Authority—to remove illicit content such as hate speech, terrorism-related material, and child exploitation, and to impose fines up to 10% of platform revenues. The measure is included in two bills regulating digital services and competition, already presented to major tech companies during a meeting at the presidential palace.

LEGISLATIVE RADAR

PL 4160/2025

Establishes a new legal framework for the sharing of electricity poles between distribution companies and telecommunications providers. Requires utilities to grant, for a fee and under regulation by Aneel and Anatel, the use of space for installing cables and equipment, subject to technical and safety standards. Also creates an independent concessionaire and a private advisory entity to support regulation, combat irregular occupations, and propose technical solutions to reduce accidents, visual pollution, and expand access to high-speed internet.

PL 4148/2025

Makes it mandatory to use a standardized numerical code for identifying outbound telemarketing calls nationwide and provides related measures.

PL 4020/2025

Imposes a 48-hour waiting period before winnings stored in virtual betting wallets can be reused for new bets, aiming to reduce impulsivity and addiction.

PL 3967/2025

Amends the Internet Civil Framework (Marco Civil da Internet) to require explicit identification of content generated or manipulated by artificial intelligence, to ensure transparency and combat disinformation.

PL 3879/2025

Ensures preservation of accounts of candidates, parties, and elected officials on digital platforms during election periods, prohibiting suspension, blocking, or deletion except in expressly defined cases. Allows removal only by judicial order limited to serious crimes (heinous crimes, child sexual exploitation, human trafficking, terrorism). Platforms that fail to comply face sanctions including fines up to 20% of revenue, immediate reinstatement of accounts, and damages.

PL 3923/2025

Regulates the profession of digital influencer, recognizing it as formal work. Defines roles, rights, and obligations, requiring truthful information, respect for human dignity, responsibility over content, and specific safeguards for child-oriented material. Prohibits prejudiced, violent, or illicit content, as well as promotion of harmful practices, with sanctions up to banning the influencer from continuing the activity.

PL 3901/2025

Creates the "Social Responsibility for Digital Platforms Law" (LRSPD), applicable to platforms with over 1 million users in Brazil. Sets principles of algorithmic responsibility, disinformation control, vulnerable group protection, and transparency in moderation and advertising. Requires quarterly reports, ad labeling, restrictions on harmful ads to minors, and alerts for excessive screen time. Provides sanctions of up to 2% of revenue (capped at R$ 50 million per infraction) and establishes the National Council for Digital Responsibility.

PL 4135/2025

Amends the General Data Protection Law (LGPD) to require digital platforms with more than 3 million users to undergo mandatory annual audits. These audits must cover the commercialization of personal data, civil liability of platforms, and algorithmic transparency, even in the absence of risks or irregularities.

PL 4126/2025

Prohibits educational institutions from sharing images that identify children's faces on social networks and provides related measures.

PL 4030/2025

Amends the Penal Code and the Child and Adolescent Statute (ECA) to classify as a crime the digital sexualization of children and adolescents, even without explicit nudity. Establishes imprisonment of 4 to 8 years and fines, with harsher penalties if content is shared on digital platforms. Holds parents, guardians, influencers, and adults accountable if they induce, allow, or omit intervention in such exposure, and sets preventive measures, educational campaigns, and platform liability.

PL 3986/2025

Prohibits monetization of illegal or exploitative content involving children and adolescents, requires removal within 24 hours, technological prevention of reuploads, creation of a "Child Alert" channel, and penalties of up to R$ 50 million for non-compliant platforms.

PL 3991/2025

Amends the Penal Code and the ECA to establish a penalty banning the use of social media, cell phones, and the internet for individuals convicted of digital crimes against children and adolescents, for the same duration as their prison sentence.

PL 4014/2025

Defines as a crime (3 to 6 years' imprisonment) the production or transmission of content depicting children and adolescents in a sexualized adultization context. Also prohibits monetization/boosting of such content and holds platforms accountable if they fail to remove it after notification.

PL 4015/2025

Requires age verification for access to online sexually explicit content, with a "double anonymity" system to protect privacy. Sets technical requirements, a 180-day adaptation period, and fines of up to R$ 50 million per violation.

PL 4022/2025

Prohibits the use of algorithms and recommendation systems for sexual content involving children and adolescents. Creates the Digital Compliance Seal, requires audits and reporting channels, and classifies in the Penal Code the crime of "premature sexualization of children/adolescents" (2 to 4 years' imprisonment).

PL 3946/2025

Amends the Internet Civil Framework to require that minors under 16 may only have social media accounts if linked to a pre-existing account of a legal guardian. The measure aims to strengthen parental supervision and reduce risks such as exposure to inappropriate content, grooming, cyberbullying, and negative mental health impacts.

PL 3924/2025

Creates the "Felca Law," establishing protections for children and adolescents online. Requires age verification, parental consent, and mandatory access controls, and prohibits targeted advertising based on minors' data. Mandates removal of illegal content (sexual exploitation, encouragement of suicide or self-harm, school attack threats) and annual awareness campaigns. Amends the ECA (Child and Adolescent Statute) to increase penalties for digital crimes against minors, up to 40 years in cases of sexual exploitation.

PL 3902/2025

Establishes the "Right to Digital Disconnection for Children," with guidelines to limit screen overexposure among minors. It requires schools to restrict screen time in remote classes, add digital citizenship to curricula, and promote offline activities. Platforms must provide pause alerts, parental controls, respect usage schedules, and restrict nighttime notifications. Also mandates a national awareness campaign to combat tech dependence and protect mental health.

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

Mario Baldir
Lawyer

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

ALMEIDA ADVOGADOS