DIGITAL LAW

DIGITAL NEWSLETTER

14TH EDITION

Check out the latest news in this edition

ALMEIDA
ADVOGADOS

ALMEIDA
ADVOGADOS
CORPORATE LAW

DIGITAL NEWSLETTER

14TH 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!

WEAK PASSWORD LEADS TO BANKRUPTCY OF 158-YEAR-OLD COMPANY AFTER CYBERATTACK

A company with 158 years of history went bankrupt following a cyberattack that exploited a weak password. The incident exposed the fragility of the company's digital security, as its systems were compromised and critical data was held hostage. Experts stress the importance of strong information security policies, including the use of robust passwords, multi-factor authentication, and regular employee training. The case serves as a warning of the real risks that digital negligence poses to an organization's survival.

AI PLATFORM DELETES COMPANY DATABASE DURING CODE FREEZE

During a code freeze period, an AI-powered coding platform accidentally deleted the entire production database of a company. The CEO of Replit, the company responsible, publicly apologized and stated that the AI made a "catastrophic error in judgment." The incident raises concerns about the use of autonomous systems in critical environments and highlights the importance of human oversight mechanisms. The company is reviewing its protocols to prevent similar failures in the future.

USER CYBERSECURITY SPENDING TO REACH USD 213 BILLION IN 2025

According to Gartner's projections, global end-user spending on information security is expected to reach USD 213 billion in 2025, up from USD 193 billion projected for 2024. Growth is driven by the increase in cyber threats, the growing adoption of artificial intelligence—by both companies and criminals—and the shortage of skilled professionals, which leads many organizations to rely on external providers. Most of the investment will go toward software security and outsourced services, with a particular focus on protecting applications and AI-powered cloud workloads. Spending is expected to remain on an upward trend in the coming years.

PHISHING CAMPAIGN TARGETS MOZILLA DEVELOPERS

Mozilla has warned of a phishing campaign aimed at Firefox extension developers. Fraudsters send fake emails imitating official communications, claiming that developer resources must be updated to remain functional. The messages contain links to fake pages designed to steal login credentials. There is at least one confirmed victim, and compromised accounts could be used to distribute malicious extensions to millions of users.

93% OF EMPLOYEES FEED DATA INTO AI TOOLS WITHOUT APPROVAL

A ManageEngine study revealed that 93% of employees use AI tools without company approval, often inputting internal and confidential data, increasing the risk of leaks due to lack of oversight and clear policies.

Additionally, 60% have been using such tools for over a year, and many have already sent confidential client information (32%) and internal company data (37%) without explicit authorization. In contrast, 63% of IT managers see data leaks as the main risk, while 91% of employees believe there is little or no risk, focusing instead on productivity gains.

LAZARUS GROUP COMPROMISES OPEN-SOURCE REPOSITORY

The Lazarus Group, linked to North Korea, carried out an espionage campaign compromising open-source code repositories on popular hosting platforms. They inserted malicious packages that steal credentials, install backdoors, and maintain persistent control over systems — potentially affecting up to 36,000 developers since early 2025, with 234 packages blocked by Sonatype as of July this year.

The fake packages closely mimic legitimate tools to trick developers and automated installation systems. Instead of conducting visible and destructive attacks, Lazarus now focuses on quiet, long-term infiltration of the open-source software supply chain to maintain hidden access for longer.

RECORDS INDICATE SCHEME WITHIN SÃO PAULO MILITARY POLICE TO TAMPER WITH BODY-WORN CAMERAS

The São Paulo Police Internal Affairs Division has requested an investigation into suspicions that a Military Police major manipulated and deleted footage from a body-worn camera recorded during an operation in Santos that resulted in the death of a man in 2024. System records show changes to metadata and deletion of the video, raising doubts about the integrity of the system and prompting an internal inquiry as well as a request for investigation by the Public Prosecutor's Office.

USING AI-POWERED CAMERAS TO ESTIMATE AGE IN TOBACCO SHOPS IS BANNED, SAYS CNIL

France's data protection authority, CNIL, has ruled that using "augmented" cameras with artificial intelligence to estimate customers' ages in tobacco shops is illegal under the GDPR. These devices scan faces in real time, showing a green or red light to indicate adult or underage status, but analyze all people in view without storing images or data.

The CNIL found the technology unnecessary, disproportionate, and a risk for excessive surveillance—especially since shopkeepers still request official ID even after the automated analysis. It also warned about errors and bias in algorithms, which could wrongly block legal sales or fail to prevent underage purchases.

DENMARK LEADS GDPR SIMPLIFICATION PROPOSAL BUT WARNS SCALEUPS MUST NOT BE LEFT OUT

At an informal meeting of EU justice ministers in Copenhagen, Denmark pushed for targeted amendments to the GDPR to make it more accessible for small and medium-sized enterprises (SMEs) and fast-growing companies known as scaleups.

Suggestions include reducing the requirement for detailed reporting for low-risk companies, simplifying or waiving the need for Data Protection Impact Assessments (DPIAs), and requiring that complaints be handled internally before going to authorities.

The European Commission supports targeted adjustments rather than a complete overhaul of the law, focusing on companies with up to 750 employees. Experts warn that limiting measures to SMEs could leave out scaleups—key players in Europe's innovation and competitiveness.

OPENAI CEO WARNS BANKS OF LOOMING AI FRAUD CRISIS

OpenAI CEO Sam Altman warned at a Federal Reserve conference in Washington that the use of generative AI in scams—particularly voice cloning—poses a real and imminent threat to the financial system. He called it "insane" that banks still rely on voice authentication, which AI can now easily replicate, potentially enabling unauthorized transfers.

Altman said AI has already defeated almost all verification methods except passwords, leaving the financial sector vulnerable to sophisticated fraud. He emphasized that this failure requires urgent reformulation of authentication systems and suggested working with regulators on new security solutions. Estimates suggest 45% of financial institutions have faced AI-driven attacks in recent months.

AI TOOL REVIEWS U.S. REGULATIONS AIMING TO CUT HALF OF THEM

The Trump administration is using a tool called the DOGE AI Deregulation Decision Tool—developed by the Department of Government Efficiency (DOGE)—to analyze around 200,000 federal regulations and identify those that could be eliminated, with the goal of cutting the total by half.

The tool has already worked at the Department of Housing and other agencies, reviewing hundreds of clauses in days and helping draft deregulation decisions. Internal documents from July1 indicate up to 100,000 rules could be scrapped through this automated approach, significantly boosting the government's deregulation efforts.

SHARED CHATGPT CONVERSATIONS APPEARING ON GOOGLE, EXPOSING USER DATA

The ChatGPT conversation-sharing feature allowed chats marked as "search-engine discoverable" to be indexed by Google, making them publicly visible.

As a result, users who shared their conversations inadvertently exposed sensitive information—ranging from personal matters to professional data. While the chats do not display names, many contained identifying details. In response, OpenAI removed the feature and is working with Google to de-index the links, though cached copies may remain in search results.

SANTA CATARINA COURT OVERTURNS TEACHER'S SUSPENSION BASED ON STUDENT RECORDING

The Santa Catarina Court of Justice (TJSC) overturned an administrative proceeding that led to the suspension of a teacher, whose conduct had been recorded by a student in the classroom. The decision found that the recording was obtained without authorization and could not be used as the main evidence in the disciplinary process. The TJSC highlighted the importance of due process and the protection of privacy in the school environment. The ruling reinforces the need for caution when using evidence obtained through questionable means, especially in cases that can affect the careers of public servants.

LEGISLATIVE RADAR

PL 3610/2025

Establishes the National Policy for the Promotion of the Use of Social Technologies – Popular Science Law, aimed at fostering, recognizing, and applying low-cost, high-social-impact technological solutions, especially those adapted to the reality of Brazil's Legal Amazon and other regions of high socio-environmental vulnerability.

PL 3669/2025

Proposes amending Law 10973/2004 to expand the scope of the National Innovation Policy to include regions with low Human Development Index (HDI) and to establish Regional Innovation Centers (CIRs) as strategic instruments to support the economic and technological development of these areas, with a focus on sustainable and territorial inclusion.

PL 3641/2025

Proposes amending Law 14133/2021 (Public Procurement Law) to make it mandatory to include a QR Code on public works signage, directing any person via mobile device to an official platform with up-to-date information on the contract's execution. The QR Code must provide access to the contract and bidding number, project description, contracted and paid amounts, identification of the responsible company, schedule, amendments, accessibility data, environmental licensing, images, inspection reports, and technical documents — all in clear and accessible language.

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