

April 2026

Monthly Digital Report

Raport pregatit de Ana-Maria Anghel



Executive summary

Highlights of the previous month

What to expect this month

Executive summary

In **April**, Romania advanced a dense legislative agenda focused on cybersecurity governance, telecom regulation, public digital infrastructure, and EU-aligned consumer and data rules, with most initiatives moving toward the Chamber of Deputies for final decision.

The Senate rejected a **cybersecurity coordination bill** that would have created an interinstitutional framework under DNSC for vulnerability reporting and introduced legal protections for good-faith security research, alongside strict reporting timelines. The same chamber also rejected two proposals **restricting minors' access to social media**, which would have imposed a 16-year age limit and strict age verification and content moderation obligations for platforms.

At the same time, lawmakers continued to reshape the digital regulatory environment. A USR proposal introduced a **unified digital governance model for public institutions**, requiring centralized registers, role-based access control, interoperability, and stricter auditing obligations for public IT systems. PSD and AUR proposed **stricter consent rules for telecom operators**, reinforcing transparency and limiting dark patterns in user consent flows. At the EU level, a new regulation **tightened cybersecurity vulnerability disclosure rules**, requiring rapid patching within 72 hours and formalized coordination with CSIRTs and ENISA. ANCOM also proposed **a reform of telecom statistical reporting**, simplifying some indicators while introducing more granular technical data and reducing reporting frequency.

In parallel, the Senate adopted **a national digital design standard (SUDD) for public services**, mandating unified UI/UX principles, accessibility standards, and system-wide compliance for all government digital platforms, now under review by the Chamber of Deputies.

Looking ahead to **May**, the legislative focus shifts to structural digital infrastructure and platform regulation. The Chamber of Deputies is expected to vote on **the creation of the National Platform for Public Digital Infrastructure (PNIDP)**, a centralized registry for all state digital assets, introducing strict security, interoperability, and governance requirements across public IT systems. It may also reject a **proposed 2% tax on large digital platforms' intermediation revenues**, while the Senate is set to examine **new rules for telecom billing in foreign currencies**, requiring full transparency and conversion strictly at the official BNR exchange rate.

Overall, the period reflects a clear regulatory trend toward centralization of digital governance, stronger cybersecurity obligations, tighter platform accountability, and increased transparency across both public and private digital ecosystems.

Highlights of the previous month

(1) Cybersecurity Coordination Bill, Rejected by Senators

In April, the Romanian Senate rejected a legislative proposal put forward by members of the former governing coalition, aimed **at improving institutional coordination in cybersecurity and clarifying the legal framework for vulnerability research**. The draft would have created an interinstitutional committee coordinated by the National Cyber Security Directorate (DNSC) to facilitate cooperation, analysis, and information exchange between authorities. It also proposed amendments to the Criminal Code to ensure that good-faith cybersecurity research and vulnerability reporting would not be treated as criminal offences, provided no harm is caused, and strict safeguards are followed. The initiative further introduced a 48-hour deadline for reporting vulnerabilities and established rules on confidentiality and system protection. The proposal has been sent to the Chamber of Deputies for final debate.

Impact: These measures would require telecom operators, digital platforms, and cybersecurity providers to implement clearer internal processes for vulnerability detection and reporting, while strengthening cooperation with public authorities. At the same time, they would offer greater legal certainty for ethical hacking and security testing activities

(2) Senate Rejects Bills Restricting Minors' Access to Social Media

Additionally, **two legislative proposals to ban or restrict access to social media platforms for minors under 16 were also rejected by the senators**, both being sent to the deputies for final debate. **One proposal**, initiated by MP Raisa Enachi, sets a minimum age of 16 and requires platform providers to implement effective, proportionate, and non-discriminatory age verification mechanisms, while strictly limiting the collection of personal data to a binary confirmation of age. The **second proposal**, initiated by MP Ștefan-Alexandru Băișanu, introduces a stricter approach by prohibiting minors under 16 from accessing or creating accounts on social media platforms altogether, alongside obligations to verify age, minimize data collection, and prevent harmful or inappropriate content targeting children.

Impact: If adopted, these measures would impose significant compliance obligations on social media and digital platform providers, including the implementation of age verification systems, stricter data protection practices, and content moderation requirements.

(3) USR MPs Propose a Unified Digital Governance System

Romania could have a unified national digital governance system for public institutions, according to a new **legislative initiative** proposed by USR lawmakers. This would require all existing and new public IT systems to integrate with key national registers and a single authorization mechanism, effectively eliminating local access management. It (3)also introduces strict role-based access controls tied to

nationally defined functions, mandatory data updates within set deadlines, and automatic synchronization of access rights by IT providers. The draft also mandates full interoperability across public systems through standardized APIs, as well as logging and audit mechanisms for all digital operations.

Impact: IT service providers, software developers, and telecom or digital companies working with public institutions would face significant technical and compliance requirements. These include mandatory system integration with national platforms, implementation of standardized access controls, and deployment of interoperability, logging, and audit capabilities.

(4) PSD – AUR Propose Stricter User Consent Rules for Telecom Operators

PSD and AUR have jointly initiated a **legislative proposal** introducing new obligations for telecom operators and service providers regarding how user consent is obtained and managed. It requires that **acceptance and refusal options be displayed with equal visibility and prominence in consent banners or similar interfaces**, while **detailed preference settings must be presented separately and cannot replace the main choices**. It also exempts cases where data access is strictly necessary for transmitting communications or providing services explicitly requested by the user. The proposal bans pre-ticked boxes, default-enabled consent, or misleading design practices, and requires that users can withdraw consent at any time through an equally simple mechanism. Operators must also be able to demonstrate valid consent and its timing, in line with data protection rules.

Impact: If adopted, the proposal would directly affect telecom operators, internet service providers, and digital platforms operating in Romania by tightening consent management requirements. Companies would need to redesign user interfaces, consent flows, and backend systems to ensure full transparency, equal choice presentation, and auditability of consent records.

(5) EU Sets Stricter Rules for Delayed Cyber Vulnerability Disclosures

In April, the EU institutions adopted a **regulation** introducing **detailed conditions and timelines under which cybersecurity-related reasons can justify delaying the public disclosure of vulnerabilities and security incidents** affecting digital products. The framework places greater responsibility on manufacturers and cybersecurity teams, requiring that mitigation measures or security patches be made available within 72 hours of notification to prevent premature information sharing between CSIRTs. It also establishes strict procedures for coordinated vulnerability disclosure, allowing delays only when justified by security needs and subject to oversight by national CSIRTs and ENISA. These provisions will enter into force on 10 May 2026 and will be directly applicable across all EU Member States.

Impact: For digital, telecom, and cybersecurity companies, the regulation significantly tightens incident response and vulnerability management obligations. Operators will need to ensure rapid patch development (within 72 hours), maintain alternative reporting channels, and adapt to varying disclosure timelines across EU markets.

(6) ANCOM Reshapes Telecom Reporting Framework

ANCOM has proposed a new **draft decision** that **restructures the statistical reporting obligations for providers of public electronic communications networks and services** in Romania. It introduces a revised and expanded set of statistical indicators, while other indicators are removed or simplified, including data on service churn and fixed-line service metrics. The decision eliminates one of the three annual reporting cycles, consolidating data collection into two main semi-annual submissions, with new deadlines set for August and February, depending on the dataset. A transitional regime applies for mid-2026 reporting, and the current framework under ANCOM Decision No. 333/2013 will be repealed as of 1 July 2026.

Impact: For telecom operators and digital infrastructure providers, the new framework changes both the scope and rhythm of regulatory reporting. Companies will need to adapt internal data collection systems to capture more granular technical and network-level indicators.

(7) Senate Adopts National Digital Design Standard for Public Services

Finally, the senators have adopted a draft bill initiated by USR **establishing the Unified Digital Design System (SUDD)**, a national framework for standardising the design and implementation of public digital service interfaces. The bill applies to all public authorities and public-law bodies, requiring full compliance for new services and major upgrades, while existing digital services must be aligned within two years of entry into force. SUDD requirements will also be integrated into all future public procurement processes for digital systems. Limited temporary exemptions of up to 12 months may be granted in cases of technical complexity, national security systems, or ongoing migration projects. Now, the bill is in the final debate of the Chamber of Deputies.

***Impact:** For IT vendors, telecom operators involved in public sector infrastructure, and digital service providers, the reform introduces a binding national UI/UX and system design standard for all government-facing digital products. This would require significant redesign of existing platforms, stricter compliance in public procurement bids, and alignment with centralized technical and accessibility standards.*

What to expect this month

(1) Deputies to Adopt Unified Registry for Public Digital Infrastructure

In May, the Chamber of Deputies (decisional forum) is expected to adopt a **USR-initiated bill** establishing **the first unified legal framework for the registration, management, and security of Romania's public digital infrastructure**. The bill creates the National Platform for Public Digital Infrastructure (PNIDP), a centralized registry covering all digital assets used by public institutions, including domains, websites, applications, software licenses, IT equipment, and publicly funded digital projects. The framework also introduces standardized technical security requirements, interoperability obligations, unique persistent identifiers for digital resources, and a mandatory digital officer role in each institution.

Impact: For IT vendors, telecom operators working with the public sector, and digital infrastructure providers, the proposal introduces a highly structured governance and compliance framework for all public digital assets. Companies will need to align systems with national registry requirements, interoperability standards, and strict security baselines such as encryption, MFA, and cloud integration rules.

(2) Deputies Could Reject 2% Tax on Large Digital Platforms

In May, the Chamber of Deputies, as the decision-making body, may reject a legislative proposal introducing **a temporary contribution on revenues generated from digital intermediation services in Romania by large online platforms**. It targets platforms with global revenues exceeding €750 million and applies a 2% levy on gross commissions earned from transactions linked to Romania, regardless of the provider's legal structure or tax residency. The measure defines digital intermediation broadly, covering services that connect users and facilitate transactions, and requires quarterly declaration and payment, with foreign companies obliged to appoint a fiscal representative in Romania. It is intended as a temporary measure, to be reassessed in line with international tax developments, including OECD Pillar 1 reforms, and would enter into force nine months after publication if adopted.

Impact: For large digital platforms operating in Romania, the proposal would introduce a direct tax on marketplace and intermediation revenues, increasing operational costs and compliance requirements. It could affect pricing models, platform margins, and cross-border structuring strategies, while also requiring enhanced tax reporting and local representation.

(3) Senate to Vote on EU-aligned Billing Rules for Telecom Contracts in Foreign Currencies

At the same time, the Senate is expected to vote, as the first chamber, on another USR-initiated **legislative proposal**, this time establishing **clear rules for billing telecom contracts concluded in euros or other foreign currencies**. It requires electronic communications providers

to inform users before contract signing that all invoices will be issued in Romanian lei, using the NBR exchange rate from the previous working day, without additional fees, margins, or commissions. It also mandates that all invoices must be issued exclusively in RON at the official NBR rate, ensuring full transparency and preventing hidden currency conversion costs. Non-compliance with these rules would trigger sanctions under a newly introduced legal provision.

Impact: For telecom operators and digital service providers, the measure standardises currency conversion practices and removes flexibility in billing foreign-currency contracts. Companies will need to adjust billing systems, pricing engines, and customer communication flows to ensure strict alignment with daily NBR exchange rates and eliminate any supplementary conversion fees.