List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

Access & literacy | Development of IG ecosystem | Human rights & data protection | Innovation and economic issues
Media & content | Cross cutting / other issues | Security and crime | Technical & operational issues

				Categories the proposal is related to								
ID	Submitted by	Affiliation	Stakeholder Group	Access & literacy	Development of IG ecosystem	Human rights & privacy	Innovation & economic issues	Media & content	Other category	Security & crime	Technical & operational issues	Suggested issue
1	Babatunde Onabajo	ChurchMapped Limited	Private sector	■			■					Artificial intelligence (AI) has been in the news quite a lot recently, and some of the latest developments in the space such as large language models (LLMs), foundation models and transformers have had profound impacts on society already. The issue is whether the education system is currently equipped to handle this? Firms in the technology sector rely on universities and other places of learning to provide an accurate assessment of a graduate's capabilities so that this can be used to better understand a candidate in the hiring process. Yet, large language models make it relatively easy for unscrupulous individuals to pass off work generated as their own when it is not. Furthermore, so-called "AI detection" has not been empirically verified and reliance on them raises the risk of falsely accusing a student of academic misconduct. How can the education sector be better placed to address the challenges of LLMs and other forms of artificial intelligence, and can companies in the tech sector help in any way?
2	Amali De Silva-Mitchell	IGF Dynamic Coalition on Data Driven Health Technologiesiesogies	Other			■	■				■	What is the status of the uptake of AI in the EU Healthcare space? What are the current applications in use and what is the future EU vision with timeline?
3	Amali De Silva-Mitchell	IGF Dynamic Coalition on Data Driven Health Technologiesiesogies	Other			■	■				■	What is the status on the use of robots in the EU? What in particular is the used of robots in Healthcare?
4	Aldan Creo	JEF Galicia	Civil society							■		Jailbreaks target AI systems to bypass their security measures. For example, a chatbot may be designed to refrain from answering "Identify the vulnerabilities in this code and develop an exploit to steal the data of users." However, a successful jailbreak deceives it into responding to the query, a significant security risk. Designing effective jailbreaks is challenging, but there have been some successful creations and proposed techniques to facilitate their development (https://arxiv.org/pdf/2308.03825, https://arxiv.org/pdf/2307.08715, https://arxiv.org/pdf/2407.04295). While most providers eventually update their systems to prevent specific instances of jailbreaks, there exists a certain period of time during which they can be utilized to exploit the system. Perhaps more troubling is that some jailbreaks have captured considerable attention online, being disseminated on social media and other platforms. This resulted in periods when a significant proportion of users exploited jailbreaks to engage in malicious activities (https://arxiv.org/pdf/2405.01470), and also developed more sophisticated versions of such, thereby complicating the patching process. Currently, there is no regulatory framework in place governing the dissemination of jailbreaks online. However, it is becoming increasingly urgent to discuss whether such a framework should be established. How should the balance be struck between the right to freedom of expression and the necessity to safeguard AI security?
5	Mehedi Hasan	RMG Sustainability Council (RSC)	Civil society	■		■	■					Energy Security and Transition to Renewable Energy is a pressing issue for Europe due to its reliance on imported fossil fuels and the need for a sustainable, stable energy supply. Recent geopolitical tensions, particularly the war in Ukraine, have disrupted energy markets, exposing vulnerabilities in Europe's energy system. This has underscored the urgency of transitioning to renewable energy sources to achieve energy independence and meet the EU's climate goals under the European Green Deal. However, this issue is part of a broader, complex problem that intersects with climate change, economic resilience, and geopolitical stability. Europe's dependence on fossil fuels not only hampers its ability to reduce emissions but also makes it vulnerable to supply shocks and price volatility. The rapid adoption of renewable technologies is necessary, but it requires addressing infrastructure challenges, such as developing efficient energy storage and modernizing grids. Social and political dimensions also play a critical role, as regions and industries dependent on fossil fuels face economic risks, necessitating policies to ensure a just transition for affected communities. Addressing this issue is vital for Europe's long-term stability and prosperity. Achieving energy security through renewable energy not only mitigates geopolitical risks but also positions Europe as a global leader in sustainable development, driving innovation and setting an example for other regions to follow.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

Access & literacy · Development of IG ecosystem · Human rights & data protection · Innovation and economic issues
Media & content · Cross cutting / other issues · Security and crime · Technical & operational issues

6	Alessia Sposini	Youth IGF Italy	Civil society							■	■		For a European Digital and Cyber Strategy 2030 In recent years, the European Union has been enacting a series of both cross-sectoral and sector-specific legislation (e.g., NIS2, DORA, AI Act, CRA) to safeguard the digital and cyber domain. The main risk is a regulatory overflow that burdens national governments with the task of strategically prioritizing requirements and accordingly investing to boost national capabilities. Moreover, private sector entities are left alone to comply with several, sometimes overlapping, requirements. All this translates, on a larger scale, into two main pain points: increased costs for national governments due to different waves of overlapping regulations, and a lack of an EU shared strategic approach due to nation-specific implementations of the EU legislative framework. On a smaller scale, the private sector is facing increased costs due to continuous new regulatory requirements, a lack of specific competencies to enact such requirements in practice, and a lack of a clear and prioritized strategic roadmap to ensure overall organizational resilience. To mitigate the aforementioned risks, there is an urgent need for an EU shared strategic approach that not only sets long-term goals on specific cybersecurity or emerging technology issues but also covers the priorities of the entire digital and cyber landscape, guiding national states and, consequently, the private sector, to avoid the duplication of efforts (both financial and human).
7	Anelia Dimova	Media 21 Foundation	Civil society	■	■	■							We would like to present a project results: Bulgarian Ministry of Electronic Governance/MEG and a Consortium comprising of 3 NGOs implement a project: Conducting a national assessment of the development of the Internet in Bulgaria through the adopted framework of UNESCO Internet universality indicators in the context of the Fourth National Action Plan, within the framework of the international initiative "Open Government Partnership", thematic area - Transparency and access to information
8	Torsten Krause	Stiftung Digitale Chancen	Civil society	■		■							The Australian Goverment decided to ban children below the age of 16 from certain social media providers. Some applaus them for the strict and straigt decision to protect children. Other refrain and call it a massive intervention in the right of the child of access to the media. What are the stances of european stakeholders? Would such a ban a good solution for children in Europe too or do we appreviate other answers?
9	Babar Khan Akhunzada	SecurityWall	Technical community			■					■		The rise of AI-driven cyber threats, such as automated phishing, deepfake-enabled fraud, and AI-powered malware, poses a significant challenge for Europe's cybersecurity framework. These threats can bypass traditional security measures, making it essential to adopt advanced detection and mitigation strategies. As AI technology becomes more accessible, adversaries are leveraging it to launch sophisticated attacks. Europe must address these threats by developing regulatory frameworks for AI use, investing in AI-driven defensive systems, and fostering collaboration between member states to share intelligence and best practices. This issue is critical to ensure the safety of digital infrastructure, citizens, and businesses in the region. This issue intersects with the EU's broader goals of digital sovereignty and cybersecurity strategy, aligning with efforts like the Cyber Resilience Act and NIS2 Directive. Addressing it would also complement innovation in AI regulation under the AI Act.
10	Eleftherios Chelioudakis	Homo Digitalis	Civil society			■	■				■		Access to economic participation through payments is a fundamental human right. Yet, many modern digital payment systems often act as tools for corporate surveillance, extracting and monetizing personal data while excluding marginalized groups. This makes reimagining digital payments to prioritize human rights, privacy, and accessibility an urgent need. This challenge aligns with three core European principles: Privacy as a Default in Online Payments: Current systems frequently compromise user privacy, enabling extensive surveillance infrastructures. Privacy-by-design solutions, however, can uphold EU fundamental rights, fostering trust and safeguarding personal data within the digital economy. Open-Source as a Foundation for Trust: Proprietary platforms limit transparency and user empowerment. Open-source technologies, supported by initiatives like the European Commission's NGI programs, ensure accountability and foster innovation. Strengthening incentives for such projects is crucial to building resilient digital ecosystems. Accessibility and Inclusion: Millions remain excluded from digital financial systems due to high costs, complex interfaces, or structural barriers. Inclusive design can close these gaps, ensuring equal participation while adhering to EU regulations on data protection, anti-money laundering, and tax compliance. Finally, this issue ties directly to the Digital Euro legislative initiative, offering an opportunity to embed privacy, openness, and inclusivity into the next generation of digital payments.
11	Mathea Essinger	Fellowship BMDV	Other			■		■					Status quo of the DSA enforcement in Germany and policy recommendations for the improvement of its framework with a focus on the protection of vulnerable groups
12	Amali De Silva-Mitchell	IGF DC DDHT	Other				■	■			■		What differences exist for supporting ehealth for the youth group VS children, adults and elderly ? What should we be aware of ?
13	Jorge Cancio	Bakom	Government						■				The Sao Paulo Multistakeholder Guidelines (SPMG) offer specific guidance to improve multistakeholder processes. NRIs and Eurodig can lead by example by analyzing its own processes in light of the SPMG and showcasing the results of such evaluation

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

14	Edan Ring	Israel Internet Association (ISOC-IL)	Civil society	■		■		■				Digital Divide in Multicultural Societies The digital divide in multicultural societies is one of the most pressing challenges of the modern digital era. Both in Europe and in Israel, closing this divide presents a crucial catalyst for socioeconomic advancement across diverse communities and populations. With a population of 447 million people across 27 member states, the EU faces unique challenges when addressing digital inequalities among its multicultural population, including linguistic minorities, migrant communities, and economically disadvantaged groups. Similarly to other multicultural societies, in Israel ISOC-IL identifies the digital divide across a wide range of levels and fields, revealing how digital exclusion and inequality manifests throughout society. This includes data collection and analysis on internet access, digital literacy, and online safety patterns among Israel's diverse populations, including Arab society, ultra-orthodox Jewish communities, senior citizens, and various socioeconomic groups. The upcoming EuroDIG presents a crucial opportunity to examine digital divides through cross-cultural, evidence-based research. Comparing experiences and data across different multicultural societies can inform more effective policymaking and practical solutions. This exchange of knowledge and methodologies at EuroDIG can help develop more nuanced, culturally-sensitive approaches to bridging digital gaps across Europe's diverse communities.
15	Nitsan Yasur	Israel Internet Association (ISOC-IL)	Civil society		■			■		■		Online Safety and Content Moderation by Digital Platforms The challenges of online safety and platform accountability become particularly acute during times of crisis and conflict. Social media platforms face unprecedented challenges in handling surges of harmful content, disinformation, and coordinated inauthentic behavior, while maintaining user safety and information integrity. Recent conflicts highlight weaknesses in the platforms' ability to respond effectively to emergency situations, particularly regarding content moderation, response times, and consistent policy enforcement. Civil society organizations play a crucial role in this landscape, serving as independent watchdogs and first responders. Positioned between state regulation and market interests, these organizations often lead efforts to counter disinformation, protect vulnerable populations, and advocate for greater platform accountability. The upcoming EuroDIG presents a vital platform to examine these challenges and share cross-cultural experiences in addressing online threats during crises. This exchange can help develop more effective approaches to platform accountability across Europe's diverse communities.
16	Anna Lob	D64 – Zentrum für digitalen Fortschritt	Civil society	■	■							The issue I want to propose is the question of how we can increase citizen participation in topics relating to internet governance and digital policy. Citizens play a huge role in shaping the internet as a space where everybody feels welcome and where you do not have to be afraid of fraud or violence. There are lots of good practice examples from different stakeholders like civil society, businesses and governments on how to bring citizens in contact with topics of internet governance.
17	Miguel Vidal	Deutsche Telekom	Private sector		■		■					"Internet Fragmentation, 30 Years After" Thirty years after the term "Internet fragmentation" first entered the discourse, this concept now captures a reality marked by profound shifts and new challenges. Initially envisioned as a unified global network, the Internet today faces a range of forces pulling it apart—from government-imposed firewalls and regulatory barriers to the rise of large private networks owned by major tech companies. These private ecosystems often operate in parallel to the open Internet, concentrating data flows, services, and power within a handful of corporate platforms. This panel will examine the evolution of Internet fragmentation, tracing it from early warnings to the complex geopolitical, economic, and technological realities shaping it today. What are the implications of this fragmentation for global connectivity, innovation, and individual freedoms? How do isolated national networks and corporate “walled gardens” impact openness, interoperability, and competition? Finally, the panel will look forward: What does the future hold for the Internet’s original vision of global unity in an era defined by competing interests? We will explore strategies to preserve openness and cooperation while addressing legitimate concerns around security, sovereignty, and privacy in an increasingly fragmented landscape.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

18	David Frautschy	Internet Society	Civil society			■					■	Age verification National regulators across Europe are assessing technical solutions to implement age-appropriate measures in recently passed online safety regulation. Key challenges include establishing proportionate age checks for online services based on risks to users, protecting children's rights, and continued compliance with data privacy regulations. Debate on how to further protect children online continues in the European Parliament. Brussels considers action as national regulators develop age-assurance standards. Meanwhile in the UK, age verification requirements are implemented by regulator Ofcom under the Online Safety Act beginning in January 2025. Youth online safety regulators around the globe are assessing similar challenges to implementing age-appropriate protections online. In November, Australia passed a ban on social media for young people under 16 years old. France already has such an age limit in place and Sweden is considering a similar social media age limit. There are calls for a bloc-wide solution to an age limit and the Commission closed a tender on "an age verification solution" this past fall. No technical standards have been developed and further policy and technical work is needed to assess and develop effective, privacy-protective, and holistic approaches to safeguard Internet users. Restrictive age verification policy risks fragmenting the Internet across national borders. What is the path forward to protect users and an open Internet?
19	David Frautschy	Internet Society	Civil society			■					■	Negative impacts of client-side-scanning proposals: Conversations surrounding the EU "Child Sexual Abuse Regulation" are ongoing. The European Parliament has agreed on a position that would exclude private messaging from the scope of the regulation in the name of protecting encryption and preventing general monitoring. Meanwhile, the Council of the EU has so far failed to reach a common position. Both the Belgian and the Hungarian Presidencies, responsible for leading negotiations on the file within the Council of the EU, attempted numerous votes on the file during their sixth-month mandates. These votes have been unsuccessful, as a sufficient number of member states have, among other things, expressed their concerns over how the proposal may impact end-to-end encryption and privacy. Blocking countries include Czechia, Poland, Austria, Germany, Slovenia, Netherlands, Estonia, and Finland. EuroDIG has discussed this issue during the last two years. However, at this time more EU Member States have established their position on the file which could allow for a richer debate. A recast on the "Directive on combating the sexual abuse and sexual exploitation of children and child pornography" is also no being discussed, as an alternative path to the controversial Regulation. What is it and how is it different?
20	David Frautschy	Internet Society	Civil society				■				■	Threats to the Internet: dispute settlement mechanism: During the last EuropeanCommission's tenure, we witnessed different attempts to introduce mandated payments from Content and Application Providers (CAPs) to the telecommunications operators providing Internet access services. This debate has been tagged with different names: "fair-share," "cost-sharing," "network fees," and "sender pays." The latest iteration is the requirement for a dispute resolution mechanism in the interconnection market. All these fundamentally represent the same concept: of altering the Internet's networking model. As BEREC has concluded, the Internet's interconnection ecosystem is characterized by well-functioning market dynamics with balanced bargaining powers. Similarly, the majority of stakeholders in Europe have pointed out how this type of regulatory intervention risks fragmenting the Internet, distorts market competition, harms consumers, and creates adverse incentives leading to a more expensive and inefficient infrastructure with poorer quality of service and higher costs. The last EC conducted two public consultations on this topic and the results were clear: most stakeholders clearly opposed this unnecessary intervention. In fact, not even among telecom operators was there a consensus, and only the largest operators supported this type of regulatory intervention. The new EC will be required to rethink the Digital Networks Act (DNA). Any recommendations must be based on evidence and stakeholder input, including EURODIG's.
21	Torsten Krause	Stiftung Digitale Chancen	Civil society	■		■		■				Age Assurance is part of a lot discussions with regard to the regulation of services. Tech companies developing and establishing new measures and tools to estimate or verify the age of users. Legislators are striving to find solutions to protect children online. And child rights organisations see both sides of a flipping coin: te opportunity to create a child approriate digital environment and the risk to restrict access of children to the internet while impairing their rights to do so. How to get a balanced approach realizing children's rights?

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

22	Natálie Terčová	IGF Czechia	Academia			■		■		■		Sharenting, the act of parents or caregivers sharing content depicting their children online, often with sensitive personal information, has become a critical issue in Europe. It intersects with multiple categories: Media & Content: The proliferation of sharenting raises concerns about the permanence of digital footprints and the unintended consequences of sharing private content. In Europe, where digital literacy and responsible content sharing are emphasized, sharenting highlights the need for awareness campaigns and education to encourage parents to consider the long-term impacts of their online behavior. Security & Crime: Sharenting increases the risk of children's images being misused for purposes such as identity theft, cyberbullying, or even exploitation. With Europe's commitment to safeguarding children online through frameworks like the General Data Protection Regulation (GDPR), this issue emphasizes the importance of reinforcing digital safeguards and encouraging parental responsibility in mitigating online risks. Human Rights & Privacy: Children's right to privacy is enshrined in both European and international human rights law. Sharenting often occurs without the child's informed consent, which could lead to violations of their autonomy and privacy. This is especially significant in Europe, where the legal landscape prioritizes data protection and upholding individual rights. The issue underlines the necessity of integrating children's rights perspectives into broader privacy discourses.
23	Michael Terhörst	Federal Office for the Enforcement of Children's Rights in digital Services	Government	■		■		■				Digital services are an important part of children's lives. Social media applications are popular for peer interaction and entertainment. Children also have a right to participation that extends to the digital space. Given the risks of using social media, to what extent can this right be restricted, thereby limiting children's access to social media? Is a ban necessary or are there other options that take into account the risks while recognising the positive aspects and opportunities of the applications? What other alternatives are there to enable children to grow up well with media?
24	Christina Fuhs	Federal Agency for Child and Youth Protection in the Media (BzKJ)	Government	■		■		■				Digital offerings play an important role in the development of values and opinions, political education and participation of children and young people. At the same time, key values and attitudes of young people can be negatively influenced by phenomena such as disinformation, deepfakes, extremism and hate speech, which can foster hostility towards democracy. It is thus important to design digital offerings in a way that supports age-appropriate participation and democratic capacities of children and young people in the digital world. An environment created and regulated by adults. Modern child and youth protection in the media means thinking from the child's perspective. In order to support children's democratic capacity and to successfully enforce their rights in the digital space, it is essential to include their perspective and to integrate their experiences and ideas into the regulatory work. Therefore, young people's participation should also be included in the discussion and development of preventive measures and their specific design and quality criteria in order to improve the effectiveness of preventive measures. Their demands for reporting and redress procedures, safe default settings and child-friendly terms and conditions are an important part of the development and implementation. It is thus an immense importance and need for more youth participation, to integrate their experiences and ideas into regulatory work and legislation at national and European level.
25	Yannic Plumpe	TUM Think Tank	Academia			■	■				■	How can Europe define a concept of digital sovereignty that is both shared and robust, while maintaining the agility needed in the age of the network society? This question lies at the heart of Europe's struggle to secure its digital future. As cloud providers dominate critical infrastructure, the balance between autonomy and global interconnectivity becomes increasingly precarious. Efforts like Gaia-X aim to reclaim control, but these initiatives often rely on underlying technologies or standards from non-European actors, raising doubts about how "sovereign" such solutions truly are. The challenge extends beyond Europe. Many nations in the Global Majority face similar dilemmas but with fewer resources to develop independent alternatives. These countries are often left to navigate a digital landscape shaped by external powers, raising concerns about equitable access, data governance, and geopolitical dependency. For Europe, defining digital sovereignty isn't just a technical issue, it's a cultural and political challenge. It requires a shared understanding of sovereignty that respects national autonomy while fostering cross-border collaboration. At the same time, it must provide a strong foundation for resilience and innovation without stifling the flexibility essential to thrive in a rapidly evolving, interconnected world. Can Europe rise to this challenge, balancing shared principles with the adaptability needed for the network society?
26	Giacomo Mazzone	Eurovisioni	Civil society		■			■				Distinguish true from false: will be still part of human rights in the world dominated by A.I.?
27	Giacomo Mazzone	Eurovisioni	Civil society		■							EuroDIG and the national european IGFs : which kind of relations in the post WSIS+20 world ?

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

28	Melodena Stephens	Mohammed Bin Rashid School of Government	Academia	■							When it comes to assessing AI literacy, existing accreditation bodies, standards, and certifications often fall short. They tend to focus on specific aspects such as legal interpretation, ethics terminology, quality management, use cases, certifications, or digital skills. These elements only address fragments of the broader AI literacy framework. Moreover, compliance with AI literacy requirements does not necessarily guarantee trustworthy AI. The rapid evolution of AI systems often outpaces regulatory developments, creating gaps in oversight. Addressing these gaps requires a more proactive approach that anticipates balancing trade-offs of future risks and opportunities. AI literacy should not be limited to AI providers and deployers as written in the EU AI Act. It should extend to a whole-of-society, whole-of-industry, and whole-of-government approach at both national and international levels, ensuring that no one is left behind. This is not just an EU issue but a global issue which is constantly evolving. The AI supply chain and its exports and impacts are seen at a global level whether it is economy, sustainability, talent, wellbeing, or impact on lives and livelihood. This is an opportunity for EU to create a "Brussels Effect" for AI literacy. We are a diverse group of professionals concerned about this issue (gender, geography, sector) that would be happy to put together a panel/workshop to discuss it. Prof. Melodena Stephens & Paola Galvez Callirgos.
29	Xingdong Fang	Zhejiang University	Civil society		■						Digital Cooperation Between China and Europe in the Context of the "Global Digital Compact" Amid complex global geopolitics, digitalization has become a key driver of global transformation and a critical focus for national development. The UN's Global Digital Compact (GDC) offers a framework for addressing challenges and setting directions in global digital governance. Within this context, China-Europe digital cooperation is crucial for advancing innovation, bridging the digital divide, and enhancing cross-border data flows, while shaping the success of global governance. The absence of unified frameworks for cross-border data flows and technical standards poses significant challenges, particularly given the differences between China and Europe in data privacy, digital sovereignty, and AI ethics. The GDC provides a platform to foster collaboration and establish clearer rules for global digital governance. Despite these differences, China and Europe share common objectives in areas like the digital economy, AI ethics, and cybersecurity. The GDC offers a space for dialogue to align efforts and address mutual concerns. Key areas for China-Europe cooperation under the GDC include Data Governance, Ethical AI Development and Cybersecurity. While challenges like competition and geopolitical differences may persist, the GDC provides a platform for China and Europe to lead in global digital governance and shape fair, transparent rules for the digital economy.
30	Karolina Gyurovszka	Martel Innovate	Government							■	What can policymakers do to increase the uptake of OSS in the EU? OSS has become a cornerstone of innovation, collaboration, and digital sovereignty in Europe. However, its widespread adoption and integration into both public and private sectors face numerous challenges. Despite its benefits—including enhanced transparency, reduced costs, and technological independence—various actors, from corporations to grassroots to public entities, remain hesitant to adopt OSS solutions. This workshop aims at answering two pressing questions.(i) How do we increase Open Source Software uptake and awareness by companies? and (ii) How do we remove existing barriers for OSS uptake in the EU? By addressing barriers to adoption and exploring actionable priorities, which also include ethics and sustainability, the session seeks to contribute to the transformation of ongoing discussions between the OSS community, industry stakeholders, EU policymakers, and end-users. Through insights gathered from this session, the workshop aims to contribute to exchanges with the European Commission's Units dealing with the European digital ecosystem, providing perspectives that reflect the real needs of OSS users. The outputs will feed into the work carried out by Martel Innovate and Digital for Planet on EU-funded projects in shaping policy roadmaps. They will directly inform projects like OpenVerse, NexusForum.EU, and NGI Commons (websites: open-verse.eu, nexusforum.eu, commons.ngi.eu), which aim to bridge the European digital ecosystem and communities with European Commission priorities.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

31	Samo Grasic	LateLab AB	Civil society		■		■		■			Emerging Governance Issues Around Satellite Internet Constellations The rapid deployment of satellite internet constellations (e.g., Starlink) has had a transformative impact on remote communities previously lacking affordable, high-speed connectivity. This progress promises to improve living standards but also exposes critical governance challenges: · Regulatory Gaps Existing frameworks are often weak or loosely enforced, creating uncertainty and potential for unchecked private sector influence. · Enforcement Difficulties The global nature of satellite networks complicates oversight, making it hard for national or regional bodies to ensure compliance. · Monopolistic Tendencies A single dominant provider can limit competition, potentially driving up long-term costs and reducing service quality. · Commercial and Proprietary Technology Reliance on private infrastructure heightens surveillance risks and restricts transparency in data handling. · Risk of Government Underinvestment in Fiber Some governments now subsidize satellite services to quickly connect underserved regions. While this addresses immediate needs, it could deter future investment in robust, community-owned fiber networks. Over-reliance on one commercial provider leaves remote and vulnerable communities exposed to service or policy changes beyond their control.
32	Alexander Generalov	Creative Commons Global Network	Civil society			■	■	■				The challenges of harmonising the provision of free access to content between different regulatory frameworks. Essentially all artificial intelligence now violates copyright law by using content without permission to learn allegedly to the extent of violating criminal law for widespread copyright infringement. In general, it is a grey area in the law. There are both prohibitions and no freedom of use and freedom to develop the industry. So many restrictions have been imposed that under a strict approach, legal artificial intelligence can only be created on the basis of public domain text and free content (e.g. through the use of Creative Commons licences). A global legal framework and a coordination organisation or coordination within the WIPO as a UN body is needed. The EU officially enacted the world's first AI Act. The CoE Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CFE No. 225) was opened for signature. On 8 October 2024, the Commonwealth of Independent States (some of whom are also in Europe) adopted a Statement. The Heads of State advocate the formation of an international system of regulation of civil artificial intelligence under the central coordinating role of the UN on the basis of the exclusive right of states to make decisions within the framework of equal and mutually respectful dialogue in accordance with international law. In Europe, it is necessary to achieve an effective and implemented legal framework so that the interests of both business and society are taken into account at the same time.
33	Rob van Kranenburg	Martel Innovate	Private sector								■	What can policymakers do to increase the uptake of OSS in the EU? OSS has become a cornerstone of innovation, collaboration, and digital sovereignty in Europe. However, its widespread adoption and integration into both public and private sectors face numerous challenges. Despite its benefits—including enhanced transparency, reduced costs, and technological independence—various actors, from corporations to grassroots to public entities, remain hesitant to adopt OSS solutions. This participatory workshop aims at answering two pressing questions.(i) How do we increase Open Source Software uptake and awareness by companies? and (ii) How do we remove existing barriers for Open Source Software uptake in the EU? By together addressing barriers to adoption and exploring actionable priorities, which also include ethics and sustainability, the session seeks to contribute to the transformation of the ongoing discussions between the OSS community, industry stakeholders, EU policymakers, and end-users. Through insights gathered from this co-creation session, the workshop aims to contribute to exchanges with the European Commission's Units dealing with the European digital ecosystem, providing grassroots perspectives that reflect the real needs of OSS users and contributors.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

34	Sardar Farman Ullah	QUAID-I-AZAM UNIVERSITY	Academia							■		Abstract: The study aims to explore killer robots' implications for the European Union. Killer robots are autonomous weapons that can kill humans without human intervention, crossing moral lines and potentially impacting human life. Protect civilians from these weapons in the European Union, collecting public opinion against them. A protective ban on offensive killer robots is crucial for setting an honorable limit to killing-yielding mechanization and regulating other robotics and emerging technology that could destabilize international peace and security. The study uses a historical and descriptive qualitative research method, collecting data through primary and secondary data sources. The researchers discuss the future outlook on legal and ethical issues, focusing on understanding the material to prevent and control killer robot systems in the European Union. They aim to collect youth ideas to ban target killing and promote the peaceful use of robotics over military use. Relevance for the European Union This study is highly relevant for Europe due to the ethical, humanitarian, legal, and societal implications of killer robots. By engaging in research, public discourse, and policy development, the EU can play a crucial role in ensuring the responsible development and use of emerging technologies while upholding human dignity and international peace and security.
35	Oksana Prykhodko	iNGO European Media Platform	Civil society		■							One Europe one Internet? Russia officially took the course on "sovereign Internet" in 2019, with a set of amendments to existing national legislation to ensure the possibility to partition the country from the rest of the Internet. It can be "national personal matter", if not for the aggression against neighbouring countries. As a Ukrainian, I can testify the attempts to ruin of the Ukrainian Internet and energy infrastructure, killing and/or invalidization of IT, ISP, energy and other heroes-professionals (after repeated bombing attacks), cyber attacks, disinformation, as well as re-routing of Internet traffic in temporarily occupied territories of Ukraine. Attempts to destroy Baltic under-sea cables, GPS blocking, campaigns on influencing election processes throughout Europe (and maybe the world) have also to be discussed. What measures (and by whom) have to be undertaken to ensure free, secure and stable internet in Europe?
36	Oksana Prykhodko	iNGO European Media Platform	Civil society		■							Multistakeholder mapping of Europe. European Internet Governance Initiatives page of EuroDIG (https://www.eurodig.org/european-ig-initiatives/) lists 33 European national initiatives (Council of Europe – CoE - has 46 member states, and two countries, which IG initiatives are listed on this page, are nor members of CoE). So, only 31 CoE members (from 46) have their national IG initiatives. From 27 members of the European Union only 18 countries have their national IG initiatives. What does it mean? What are the roles of national IG initiatives in national/European/world-wide policy making on Internet governance? On UN level? On the level of CoE? EU? RIPE NCC? ISOC?
37	Oksana Prykhodko	iNGO European Media Platform	Civil society							■		Electronic evidences of war crimes/ Evidences of electronic war crimes The only one international binding judicial document regarding cyber crimes is Council of Europe Cybercrime Convention (ETS No.185) and Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No.224). A lot of international, national, NGO and private organizations are gathering electronic (among others) evidences of russian war crimes in Ukraine (and not only). Gathering of electronic (cyber) war crimes is more difficult.
38	Alessandro De Luca	Associazione Luca Coscioni	Civil society	■	■	■						AI for Common Good Despite longlasting discussions on its ethical implications, artificial intelligence is deeply embedded in our lives. The challenge is no longer whether to adopt it, but how to ensure it serves democratic values. How can we use AI to achieve a citizen-centered society? Can the EU harness AI to empower citizens while addressing issues like transparency, data control, and equitable access? AI can facilitate popular participation, but how do we ensure that new tools are inclusive, multilingual, and reflective of Europe's diverse political and social landscape? Open-source systems and interoperable platforms could reduce dependence on tech monopolies, yet how do we balance innovation with accountability? And can the EU lead the global race with a rights-driven approach to technology? Rather than reinventing the wheel, the EU could draw on existing innovations, scaling up solutions through a multi-stakeholder approach.
39	Jessica Sanson	Associazione Luca Coscioni	Civil society	■		■		■				Civic Social Media In the context of European political debates, where misinformation and disinformation threaten democratic integrity, can civic social media be a tool for fostering trust in democracies and safeguarding the public sphere? While digital platforms increasingly shape political discourse, a space that fosters democratic participation while adhering to European values is still missing. Drawing inspiration from the Fediverse (e.g. Mastodon), can the EU create a platform that enables citizens, civil society, and political parties to engage in transparent, inclusive discussions? And may this platform support deliberative decision-making and offer an accessible, user-friendly design compliant with EU regulations like GDPR and the DSA? In this framework, AI might help analyze contributions, detect disinformation, and summarize debates. It could also provide insights into public sentiment and highlight underrepresented voices, while offering customizable discussion modules and real-time data for policy makers.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

40	Peter Koch	DENIC eG	Technical community		■						■	Recent years have seen a number of proposed or demonstrated advances to networking or network related technologies, affecting speed, bandwidth, latency,or other physical parameters. Do any of these new technologies require, imply, or even support new governance approaches? Are there governance invariants? Are there "critical resources"? What are the new or re-shaped governance questions? What are the roles of different stakeholders?
41	Carolin Kothe	/	Civil society	■			■				■	A well-functioning public sector is the backbone of Europe's economy and a key pillar of democratic governance. Many European countries—including economically strong nations like Germany—face legacy structures and sluggish processes in justice, law enforcement, and administration. These inefficiencies impede timely justice, erode trust in governmental institutions, and can weaken Europe's global competitiveness. While AI-powered tools (e.g., automated document review, predictive policing with safeguards) can accelerate bureaucratic workflows, they also raise critical questions about ethics, data security, and due process.AI is just the surface of a deeper challenge: fostering cultural transformation in public administration and redefining the identity of the public sector. The real task is balancing dynamism and stability—an intricate endeavor requiring a coordinated, multi-stakeholder approach. This includes reimagining regulatory frameworks, setting robust standards, and building civil servants' capacity for digital transformation. One powerful lever lies in defining technical standards, taking cues from the open and collaborative "Request for Comments" approach that propelled the internet's growth. By adopting similar methodologies, public administration can ensure interoperability, security, and innovation. Embedding this mindset helps bridge the gap between technological progress and effective governance—keeping Europe innovative, rights-driven, and ready for the future.
42	Andrey Shcherbovich	Free Moscow University	Academia		■	■						Given the expiration of the current mandate of the Internet Governance Forum in 2025, it is necessary to consider its extension. At the same time, there is a need for an international organization to provide a legal foundation, infrastructure, financing and organization of international interaction of stakeholders with international legal personality (the right to conclude contracts with third parties) and immunity (protection and autonomy from national laws) for all participants in processes and dialogues, communities and organizations in all member countries (for example, regional IGFs can be held by structural divisions of such an international organization). Such a configuration can solve, in particular, a number of problems and translate discussions into practice, instead of theoretical work, begin the implementation of a number of ideas that do not develop or reach a dead end without the existence of an organization and long-term financial support. International coordination is also required to encourage not a centralized vertical, but a horizontal (within countries) model of financing professional and other communities and NGOs. The two approaches (an international organization with immunity and local within-country financing of NGOs and communities) will complement each other and provide an opportunity to choose. At present, international organizations and initiatives in the field of IG do not take into account the existence of specific national laws in a number of countries and do not understand their specific application - intended or actual.
43	Benedetta Veneruso	Deloitte Italy	Private sector	■		■	■					The adoption of AI-driven decision-making systems is creating transformative opportunities while raising significant concerns about their societal and ethical implications. These systems, though promising to enhance economic growth and innovation, also risk undermining fundamental rights, fairness, and democratic values if not properly governed. This issue is part of a broader challenge: ensuring the ethical integration of AI into society while addressing its potential to exacerbate inequalities, bias, and misuse. It is interconnected with related issues such as data governance, transparency in algorithmic decision-making, and the accountability of AI systems in critical sectors like healthcare, finance, and public services. By proposing a methodology aligned with European AI legislation, we aim to assess and mitigate the risks these systems pose to individuals and communities. This approach fosters multi-stakeholder collaboration, enabling society to harness the benefits of AI while safeguarding fundamental rights and trust in technology.
44	Benedetta Veneruso	Deloitte Italy	Private sector	■		■	■					The adoption of AI-driven decision-making systems is creating transformative opportunities while raising significant concerns about their societal and ethical implications. These systems, though promising to enhance economic growth and innovation, also risk undermining fundamental rights, fairness, and democratic values if not properly governed. This issue is part of a broader challenge: ensuring the ethical integration of AI into society while addressing its potential to exacerbate inequalities, bias, and misuse. It is interconnected with related issues such as data governance, transparency in algorithmic decision-making, and the accountability of AI systems in critical sectors like healthcare, finance, and public services. We recognize the need for a methodology aligned with European AI legislation, aiming to assess and mitigate the risks these systems pose to individuals and communities. This approach fosters multi-stakeholder collaboration, enabling society to harness the benefits of AI while safeguarding fundamental rights and trust in technology.
45	Constance Weise	IEEE	Technical community				■			■		The EU Cyber Resilience Act: Challenges and Opportunities: The Act introduces requirements for manufacturers, importers, and distributors of hardware and software products with digital elements and notes harmonization with other relevant EU legislation, such as the AI Act. What are the challenges that have been uncovered and how are they being addressed to provide a safe and secure environment.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

46	Karen Mulberry	IEEE	Technical community	■							■	Follow-Up: Network Evolution: Challenges and Solutions 1 year later: One year later – issues and challenges in mastering Europe's digital infrastructure needs, what have we learned with the implementation of policy initiatives like the Gigabit Infrastructure Act aim to speed up infrastructure deployment, while the EU Commission's White Paper, " How to master Europe's digital infrastructure needs?" tackles broader challenges and opportunities in the telecommunications sector. The discussion will delve into the experiences of the last year in implementing a robust and inclusive digital infrastructure in Europe.
47	Karen Mulberry	IEEE	Technical community	■							■	Connecting the Unconnected – What's next: Rural connectivity, enabling access to reliable internet and telecommunication services is a key enabler for achieving the UN's Sustainable Development Goals (SDGs). Achieving these goals requires leveraging technology to connect under-served populations to facilitate access to information, education, healthcare, economic opportunities, and essential services. The workshop discusses a holistic approach that converges policy, infrastructure development, application deployment, standards implementation and open-source solutions to bridge the digital divide and foster inclusive growth in unconnected communities.
48	Karen Mulberry	IEEE	Technical community	■				■				Age-Appropriate Design: With the ever-expanding reach and influence of online services, and the introduction of innovative online products, the well-being and safety of users' will need to be considered as new online services are introduced. The discussion will focus on implementation requirements identified in the Digital Services Act (DSA), the EU's Audiovisual Media Services Directive (AVMSD) and General Data Protection Regulation (GDPR) and the work of the EU in developing the Age-Appropriate Design Code.
49	Paulina Popow	Polish National Research Institute NASK	Technical community	■		■						Technological accessibility for different user groups - challenges and solutions. Technological accessibility poses a number of challenges due to the need to adapt technologies to the diverse needs of users. Technologies must be designed to be accessible and user-friendly for all users, regardless of physical, economic or social constraints. An important issue is the identification of barriers and methods to overcome them. This involves establishing legal frameworks and standards to ensure the inclusivity of technologies. A proactive approach is important to ensure universal access to the benefits of technological innovation. This requires a comprehensive strategy that takes into account the needs of different groups in society at each stage of the technology life cycle - from design to implementation. Collaboration between policy makers, technology developers and user communities is essential. This effort can lead to the creation of universally adaptable technologies. In summary, technological accessibility is fundamental to our digital future. By prioritising inclusivity, we can ensure that no one is left out, paving the way for a fairer and more connected world.
50	Paulina Popow	Polish National Research Institute NASK	Technical community							■		The importance of public-private partnerships in cyber security Public-private partnerships play an important role in ensuring cyber security.One of the most important aspects is the sharing of information about threats and incidents. By working together, private companies can quickly inform government institutions of new threats, allowing them to respond more quickly and minimise damage. In turn, the public sector can provide private companies with the guidance and resources needed to strengthen their security systems. Another important element is the joint development of standards and regulations. These partnerships enable the creation of uniform standards that help secure IT systems on a large scale. Joint training and education initiatives also play an important role, raising cyber security awareness and skills among employees in both sectors. Public-private partnerships are the cornerstone of an effective cyber security strategy. By working together, sharing information and resources, as well as joint education and research initiatives, we can provide better protection against cyber threats. Such collaboration is very important to meet the challenges of today's digital world and ensure security is at the highest level.
51	Claire Patzig	Hasso-Plattner Institut, Fellowship "International Digital Policy" - German Federal Ministry for Digital and Transport	Civil society			■	■					In March 2024, the Council of the European Union adopted the Critical Raw Materials Act (CRMA) to secure and diversify the EU's supply of critical raw materials (CRMs), essential for the so-called green and digital transitions. The key objectives of the CRMA are to diversify supply chains, enhance circularity, and support innovation. It identifies 17 "strategic resources" for which demand is expected to grow exponentially. Currently, 100% of the EU's demand for rare earths is met through imports from China, 98% of boron from Türkiye, and 71% of platinum from South Africa. The new strategic targets for 2030 aim for at least 10% of annual consumption to come from domestic sources, at least 40% to be processed within the EU, at least 25% to be sourced from recycled materials, and no more than 65% of any strategic raw material to be sourced from a single non-EU country. What has changed since the adoption of the CRMA? How is the EU progressing towards these targets, and is it moving fast enough? What does this strategy mean in practice for the environment in resource-rich countries? How can ethical challenges associated with mining practices in the Global South be addressed? Additionally, how should the EU prepare for potential trade embargos, such as those implemented by China during trade disputes with the United States?

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

52	Claire Patzig	Hasso-Plattner Institut, Fellowship "International Digital Policy" - German Federal Ministry for Digital and Transport	Technical community				■			■	■	Federated Learning (FL) is a decentralized machine learning approach that enables multiple stakeholders to collaboratively train models while keeping data localized. This method is particularly suited for international collaboration, addressing critical concerns around data privacy, security, and sovereignty. From a technical point of view a standardizing of protocols and frameworks would ensure interoperability among participants and clear governance models would enhance trust among stakeholders. Those are still somewhat lacking. Moreover, how can FL be used in other domains (currently used a lot in the health care sector)? How to enable participation in regions lacking computational infrastructure?
53	Xingdong Fang	College of Media and International Culture, Zhejiang University	Civil society		■							The Brussels Effect and Digital Governance in the Global South Over the past decade, Europe has steadily advanced its digital governance, establishing a strong "Brussels Effect." Through its regulatory frameworks, Europe has shaped global digital standards and policies, exerting profound influence on multinational corporations and solidifying its leadership in global governance. This proposal explores the interplay between the Brussels Effect and digital governance in the Global South, analyzing how Europe's digital governance model provides valuable insights for the Global South to develop inclusive, secure, and trust-based digital policies. The challenges faced by the Global South differ significantly from those in Europe, particularly in terms of digital infrastructure access, digital literacy gaps, and political and economic instability. As digitization accelerates in areas like healthcare, education, and commerce, issues such as data sovereignty, privacy, and cybersecurity have become increasingly critical. The Brussels Effect offers an opportunity for the Global South to adopt Europe's experience, building tailored digital governance frameworks while avoiding fragmentation. Objectives: 1. Impact of the Brussels Effect on Global Governance 2. Role of Multilateral Cooperation 3. Capacity Building in the Global South 4. Fostering Inclusive Policies As digitization grows, the Global South faces challenges and opportunities. The Brussels Effect offers a model for inclusive governance, enabling a role in a fairer global digital order.
54	Monika Stachon	NASK	Technical community	■	■						■	The Skills Gap in Cybersecurity in the Context of New Legal Regulations in the EU. New regulations at the European Union level, such as the NIS 2 Directive, AI Act, CRA, DSA, and CSoA, are significantly reshaping the landscape of cybersecurity requirements in Member States. These regulations introduce new obligations in organizational, operational, and competency-related areas, leading to increased demand for specialists with appropriate qualifications. However, the pace at which these regulations are being introduced reveals a significant skills gap in the labor market. Many enterprises and public institutions, especially those less mature in terms of cybersecurity, lack the human resources capable of meeting the new requirements. There is a shortage of both technical experts and specialists in risk management and regulatory compliance. The key question remains: how can this skills gap be effectively addressed? Are new educational and training programs the answer? What role can cross-sector collaborations, public-private initiatives, or reskilling programs play? How can the development of competencies be effectively monitored and supported amid rapidly changing legislative requirements? The session will address topics such as the most in-demand skills in the cybersecurity job market in the context of new EU regulations, initiatives aimed at reskilling workers and preparing new professionals, and examples of best practices and strategies to support skill development.
55	Monika Stachon	NASK	Technical community		■		■				■	Perception of Artificial Intelligence Tools in Business Operations: Opportunities and Challenges As artificial intelligence tools become increasingly accessible, their potential to transform business operations is undeniable. Yet, the perception of these tools among enterprises varies significantly and often determines their adoption and integration into daily workflows. For some organizations, AI is viewed as a revolutionary enabler of efficiency, creativity, and competitiveness. For others, it may evoke skepticism, concerns about complexity, ethical implications, or the fear of replacing human expertise. These perceptions are often influenced by factors such as company size, cultural attitudes towards innovation, and the level of digital literacy. Key questions include: • How do enterprises perceive the balance between the potential benefits and risks of AI adoption? • To what extent do leadership attitudes, employee readiness, and organizational culture shape the willingness to explore AI solutions? • What role do public narratives, case studies, and peer experiences play in shaping these perceptions? This session will delve into the "soft" aspects of AI adoption, focusing on the attitudes and expectations that businesses hold towards integrating AI into their workflows. The aim is to uncover strategies for fostering a more informed and balanced understanding of AI's role in business operations, helping enterprises navigate the transition towards more intelligent ways of working.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

Access & literacy | Development of IG ecosystem | Human rights & data protection | Innovation and economic issues
Media & content | Cross cutting / other issues | Security and crime | Technical & operational issues

56	Monika Stachon	NASK	Technical community								Cybersecurity in Operational Technology (OT): Protecting Critical Systems in a Converging Landscape Operational Technology (OT) systems, which control critical infrastructure such as energy grids, transportation, and manufacturing, are increasingly interconnected with IT networks. This convergence enhances efficiency but also exposes OT systems to cyber threats traditionally targeting IT environments. Unlike IT systems, OT environments prioritize availability and operational continuity, often making traditional security measures impractical or insufficient. Key challenges include securing legacy systems designed without cybersecurity in mind, managing the unique risks posed by industrial protocols, and addressing the lack of visibility into OT environments. Additionally, the growing sophistication of attacks targeting OT necessitates tailored security approaches. Regulatory frameworks, like the NIS 2 Directive, are pushing organizations to adopt stricter cybersecurity measures, but implementation remains uneven. This session will examine critical issues in OT cybersecurity, including: • Balancing operational continuity with effective cybersecurity measures. • The impact of emerging regulations and standards on OT security practices. • Collaboration between IT and OT teams to create unified security strategies. The discussion will focus on practical approaches to safeguarding OT systems and ensuring the resilience of critical infrastructure in the face of evolving threats.
57	Emilia Zalewska-Czajczyńska	NASK National Research Institute	Technical community								The hype around the term "metaverse" and technologies such as VR and XR has long gone. However, this does not mean that their development has stopped. Work on their potential applications continues, opening up new opportunities for industry and research. Moreover, the governance of so-called "virtual worlds" and their potential to become the next generation of the web is one of the focal points of the European Commission and the Polish Presidency in 2025. Perhaps it is a good time to reflect on current developments in virtual reality and related technologies and the way forward.
58	Maria Pericas	German Federal Ministry of Digital and Transport	Civil society								Safeguarding Europe's Critical Infrastructure: Challenges, Opportunities, and Global Implications Critical infrastructure underpins Europe's economic stability, societal well-being, and security. Sectors like energy, ICT, transport, and healthcare are increasingly vulnerable to cyber threats and geopolitical tensions. This session explores how Europe can lead in defining, securing, and setting global norms for critical infrastructure protection, drawing from its diverse experiences and advanced regulatory frameworks, such as the NIS2 Directive. This session would explore how Europe can address these challenges by: - European Priorities: Highlight the key critical infrastructure sectors in Europe, such as energy, ICT, and transport, as identified in DGAP's study. - Cybersecurity Coordination: Discuss the importance of cross-border cooperation and the role of EU agencies like ENISA in addressing shared cybersecurity threats. - The NIS2 Directive: Explore how the NIS2 Directive strengthens the security and resilience of critical infrastructure across the EU. - Global Leadership: Analyze how Europe's regulatory frameworks can serve as a model for international norms and capacity-building efforts.
59	Vittorio Bertola	Open-Xchange	Private sector								Much talk has been going on in Europe around digital sovereignty and "building the EuroStack" - making sure that we have European alternatives to the dominant, oligopolistic products offered by American and Chinese tech companies. Up to now, this has led to a ton of new regulation aimed at preventing anti-competitive behaviour and opening up the markets. On the other hand, regulation alone is not very useful in the absence of successful companies that build and sell the alternative products. Public policies on this have been a failure; European projects like IPCEI-CIS and GAIA-X did not make much difference. Some hope comes from bottom-up initiatives like openDesk in Germany and La Suite Numérique in France. Is this the model to follow? Should public institutions fund or sponsor startups and private sector efforts, and how? Should funds come with governance structures attached?
60	Cristina Herrera Garcia	Adapt	Other								Explore the EU's role in advocating for a coherent global approach to AI governance, uniting the views of diverse countries and regions, including the United Nations, the EU, and non-EU countries. This involves moving beyond mere principles to focus on practical guidance. This includes leveraging the EU's position as a regulatory leader to promote European values like privacy, fundamental rights, and bias prevention, while also considering the diverse perspectives and priorities of other regions.
61	Cristina Herrera Garcia	Adapt	Other								The Global Digital Compact recognizes the importance of the OHCHR's proposed Human Rights Advisory Service. This service can provide valuable expertise and guidance to European authorities enforcing the AI Act, promoting a rights-centered approach to AI regulation and global coherence. What would this collaboration look like?

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

62	Cristina Herrera Garcia	Adapt	Other			■						The Global Digital Compact acknowledges the importance of the OHCHR's proposed Human Rights Advisory Service. This service will provide crucial advice and guidance on integrating human rights into digital technologies, including AI. To ensure its effectiveness, it's essential to address challenges related to funding, resource allocation, and maintaining a multi-stakeholder approach that includes input from tech companies. What role could Europe play to contribute to the success of the Advisory Service?
63	Cristina Herrera Garcia	Adapt	Other			■						Bias on AI systems protection Discuss the importance of avoiding unfair bias in AI systems and safeguarding human rights, not only for EU citizens but for all individuals impacted by AI systems used within the EU.
64	Cristina Herrera Garcia	Adapt	Other	■								Media literacy from a European perspective. The EU has a unique position in terms of access to the digital world. In 2023 91% of the EU population had internet access. Therefore, the focus should be on protecting users from online harms, such as through the DSA. While election misinformation is a significant concern, it's crucial to address broader issues of online manipulation and misinformation. Europe should prioritize ongoing media literacy initiatives to keep citizens informed and vigilant, even beyond election periods.
65	Peter Koch	DENIC eG	Technical community		■						■	The EU regulatory toolset consists of a layered approach with directives, regulations, implementing acts, implementation guidelines, non-binding guidelines and similar instruments at the member state level. This helps focussing on policy objectives at the higher levels and enables flexibility with implementation details. However, a multistakeholder paradox can be observed: the higher the level of detail (also perceived as proximity to "the wire"), the harder it occurs to be for those with the strategic and operational responsibility for core -- if not critical -- infrastructure to feed their expertise and experience into the process. The planning team should identify recent cases and suggest parties to analyse and help improve the situation.
66	Dennis Redeker	Internet Rights and Principles Coalition (IRPC)	Civil society		■	■		■				XR (extended reality) and "virtual worlds" develop unabated and the governance of such emerging technologies require a strong emphasis on human rights, including with impetus from European stakeholders. The "Global Multistakeholder High Level Conference on Governance of Web 4.0 and Virtual Worlds" hosted by the European Commission and the 2025 Polish Presidency of the Council of the EU will discuss these topics (including from a human rights perspective) in March/April 2025. The EuroDIG community should aim to take up the results from the conference in order to propose itself a rights-focused approach to the governance these emergent technologies.
67	Dennis Redeker	Internet Rights and Principles Coalition (IRPC)	Civil society		■	■						The Global Digital Compact has recently been agreed upon. Some elements of it are clearer than others. In the GDC, stakeholders are encouraged to endorse the Compact and commit to its principles and objectives. The United Nations has established a platform where interested parties can formally join the GDC, signaling their commitment to promoting an inclusive, open, safe, and secure digital future for all. At EuroDIG, we should discuss if EuroDIG (as an NRI) endorses, how different stakeholders can endorse and how this can matter, and, importantly, how the European and global IG community can make endorsements matter for human rights, by encouraging those who do endorse the GDC to focus on human rights, too. Another question that could be discussed at EuroDIG is how local communities/municipalities can engage in IG by endorsing the GDC (raised as a general point at EuroDIG 2024).
68	Sergey Mokhnenko	Decentralised Science (DeSci) community	Academia	■				■			■	A well-established practice in astrophysics is the open availability of data many years after analysis, thus enabling the scientific community, including researchers from developing countries, to develop. This model, in which data is made available to all researchers, helps to narrow the gap between developed and developing countries in science. However, this practice is prevalent primarily in astrophysics, and this approach is much less common in other areas of physics. It is imperative that these principles of data openness be incorporated into other scientific disciplines in the future, ensuring that scientists in countries with limited access to modern scientific experiments do not fall behind in their research. Additionally, there is a concern regarding access to international scientific organisations for students and early-career scientists, particularly those from institutions with limited connections to global scientific communities.It is recommended that clearer and more accessible procedures for attaining full membership of these organisations be established, thereby enabling any student or early-career researcher to join international scientific communities without the necessity of navigating bureaucratic processes at the university or local authority level.This would facilitate a more equitable and unobstructed exchange of knowledge among researchers globally.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

Access & literacy | Development of IG ecosystem | Human rights & data protection | Innovation and economic issues
Media & content | Cross cutting / other issues | Security and crime | Technical & operational issues

69	Pietro Migliorati	Associazione Luca Coscioni	Civil society		■	■						As digital transformation is reshaping our lives, the EU is offered the opportunity to take a pivotal role in updating global standards for democracy. Clearly, it is not an easy task to do, and the implementation of digital democracy systems requires a holistic approach. First, the digital divide ought to be tackled to address structural gaps, thus enabling eParticipation through a more accessible and affordable Internet. Second, to pursue inclusivity, any new tool should be developed embracing open-source software, interoperability, and multilingualism. Third, discussions on secure technologies to enable e-voting and increase trust in technologies should be re-opened, following in the steps of fully digitalised countries like Taiwan and Estonia. And other challenges remain, such as digital literacy gaps, the risk of exclusion, and liability of automated agents in AI-driven decision-making. However, how can democracies bend disruptive technologies to promote political dialogue, rather than fuelling polarisation and oppression?
70	Piotr Słowiński	NASK PIB	Technical community		■					■	■	Cybersecurity risk-management measures for SME's and public administration | Cybersecurity undeniably constitutes one of the most crucial elements that SMEs must ensure, regardless of the economic sector they operate in. The same applies to the public administration – its proper operations, increasingly based on the systems and networks availability and reliability, is of key importance for the functioning of the state. Failure to ensure cybersecurity exposes to financial or reputational losses, not to mention e.g. the data leakage, systems or networks disruption, or ransomware. In addition, an increasing number of regulations, such as NIS 2, integrate above sectors into the larger cybersecurity ecosystem, so far dominated by larger entities. One of the significant factors is cybersecurity risk-management measures implementation. Its primary goal is to counteract cyber threats and incidents or mitigate their negative effects. For many SME or public administration entities implementing it can be a significant challenge – organizationally, financially, and operationally. This is influenced mostly by the maturity level. This requires further experience sharing by more mature entities and countries with those less advanced, as well as increased efforts to harmonize procedures for sharing information about incidents, responding to large-scale and cross-border incidents, as well as cooperation between countries and EU institutions in countering cyber threats and thus building the resilience of the entire Union and individual member states.
71	Piotr Słowiński	NASK PIB	Technical community				■			■		AI's cybersecurity and AI in cybersecurity - challenges and opportunities for the cybersecurity landscape in incident response, countering cyberthreats and cybercrime prevention | Artificial Intelligence (AI) dual role in cybersecurity—both as a tool for defence and a potential weapon for attackers—makes it a critical area of focus, requiring further consideration on a much deeper level than before. AI is already utilised to enhance attacks, such as through AI-driven phishing and deepfakes. It can also automate malware creation, making it more difficult to detect and counteract and at the same time - more common as it is easier for even a non-technical person to develop it. But AI can also be helpful for blue teams. It can detect and analyse threats automatically or find patterns and anomalies in large amounts of data. This helps prevent threats from happening and reduce response times. The EU is integrating AI into cybersecurity strategies, with initiatives like the AI Act and H2020 projects like IRIS. This fosters collaboration and harmonizes cybersecurity practices across member states, building a resilient digital ecosystem. As it is only the beginning of the road for the EU and the world, there is a need to undertake specific actions. This includes e.g.: -tailored investment and financing for secure and human rights centric AI systems, -expanding training and skill development capabilities in the EU -collaboration and information sharing, both on the highest and lower levels -encouraging responsible and goal-oriented public-private partnerships
72	Piotr Słowiński	NASK PIB	Technical community			■				■	■	International cybercrime regulations - current state of play and the future landscape | The Council of Europe Budapest Convention on Cybercrime was the first international treaty aimed at addressing internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. However, with the rapid evolution of technology and cyber threats, there is a growing need to revise and update this convention. Discussions on the need to address the current cybercrime challenges by adopting a new landmark international regulation were brought up. One of the most recent developments in this area is the UN Convention against Cybercrime, adopted on 24.12.2024 by the UN General Assembly. The text is the result of 5 years negotiations with the input of civil society, academic institutions and the private sector. Thus, a transition point is being reached to discuss, clarify and implement new solutions in the international dimension of combating cybercrime. A series of issues need to be addressed at this stage, related to both the interplay of existing and new regulations on each other and the linkage of international regulations on regional and national ones, not only in the area of preventing and investigating crimes, but also cybersecurity and new, emerging technologies in a broader sense. Creating a harmonised system for combating cybercrime that respects fundamental rights and ensures that the objectives of pursuing and preventing cybercrime are met is a huge and significant challenge for many stakeholder groups.

List of proposals for EuroDIG 2025 *(as of 1 January 2025)*

EuroDIG
European Dialogue on Internet Governance

■ Access & literacy ■ Development of IG ecosystem ■ Human rights & data protection ■ Innovation and economic issues
■ Media & content ■ Cross cutting / other issues ■ Security and crime ■ Technical & operational issues

73	Avraham Shmulevich	Free university	Academia	■		■						The Problem of Organizing an Online University The educational process today is still based on the same principles that universities were founded on more than 1,000 years ago. Most lectures are delivered orally by a teacher to students sitting in a physical classroom, with minimal use of modern technologies. To study, students are required to reside in a specific location. In the 21st century, this approach is hopelessly outdated. It is essential to develop an online education project that fully utilizes modern Internet technologies and is based on new principles, tailored to the needs of today's world.
74	Avraham Shmulevich	Free university	Academia	■		■				■		The problem of access to content for divided peoples. Internet as a factor of survival and preservation of national identity for diaspora and divided peoples. Europe has become home to many divided peoples. This problem has become particularly acute in recent decades. Diasporic and divided peoples are peoples who have no statehood or live in several states. They face many challenges and difficulties in preserving their national identity and language, establishing contacts with members of their own ethnicity, facing the risk of losing their language, traditions, and often facing discrimination and persecution. The Internet provides unique opportunities to overcome these challenges. Namely: Language and cultural preservation; Supporting national identity; Social connections; Human rights and political activism. Online platforms allow diasporas to create virtual communities, use the Internet to mobilize their members to defend themselves against discrimination. However, there are a number of challenges: Language barriers. Many resources are only available in a few major languages. Unequal access to the Internet; Some diaspora members lack internet skills; Restrictions on the internet in a number of countries; Issues of divided peoples require special attention when developing Internet governance policies. Strengthening digital connectivity between diaspora communities contributes to a more inclusive society in which every culture and identity finds its place.
75	Avraham Shmulevich	Institute of Eastern Partnership	Civil society	■		■		■				The Internet as a Platform for Interreligious Dialogue The internet has the potential to foster interreligious dialogue, connecting people of different faiths and promoting mutual understanding. However, several issues hinder its effectiveness: 1. Misinformation and Stereotypes: False or biased content spreads easily, reinforcing religious stereotypes and fueling intolerance. 2. Polarization and Echo Chambers: Algorithms often prioritize divisive content, limiting exposure to diverse perspectives and stifling dialogue. 3. Anonymity and Hate Speech: Online anonymity enables hate speech and reduces accountability, undermining respectful communication. Solutions: 1. Education and Awareness: Digital literacy programs can teach users to critically assess content, reducing the impact of misinformation. Interfaith organizations should develop accessible resources to counter stereotypes and promote understanding. 2. Platform Responsibility: Social media platforms must enhance content moderation, combining algorithms and human oversight to combat hate speech while fostering respectful discussions. 3. Intentional Dialogue Initiatives: Virtual interfaith forums, webinars, and collaborative projects can create safe spaces for sharing beliefs and building trust.