List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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	Sivasubramanian Muthusamy	Nameshop	Private sector	■	■		■					This is indeed a huge problem and seen as an unsurmountable challenge - historically, for a very, very long time. There are gross imbalances in a wealthy, very wealthy world, between the rich and poor, between the educated and uneducated, between the privileged and unprivileged; While the variations in level (or classes) are natural and perpetual, at various points of time, these differences are wide, with the less fortunate population living a life of scarcity and insufficiency; This can change, refugees can live, poor can live away from squalor and free of hunger, there can be water to drink and food to eat for every human; This can happen without depriving the wealthy of their wealth or the privileged of their respect, there are solutions that the Internet technologies and emerging technologies have brought about, but still not so well defined, still not attended to; Some of these solutions arise from older notions of goodness such as cities of refuge, charity, kindness, all of which can be channelised in a coordinated manner for amplified, exponential effect. Would Eurodig rephrase this into today's language of government and the language of business and address this theme in a manner that it emcompasses economic prosperity, reasonable good education by good actors, shelter, food and water and well being ?
2	Amali De Silva-Mitchell	IGF DC DDHT	Other				■					How does the internet support farming / agriculture? What Innovation is taking place ?
3	Amali De Silva-Mitchell	IGF DC DDHT	Other				■					What the advancements in healthcare such as eye surgeries and brain to glasses seeing ? This relates to complex sensing in the visual technology space
4	Amali De Silva-Mitchell	IGF DC DDHT	Other						■			What tech and internet solutions are being used for climate change monitoring? Are we prepared for dealing with climTe disasters such as flood and fire ? How will the disabled be taken care of in these situations?
5	Grigor Nersisyan	Center for Public Finance and Personal Data Protection Monitoring, Education NGO	Civil society							■		AI Transparency & Accountability in Public Sector Use Suggested issue: Ensuring transparency and accountability in the use of artificial intelligence by public sector institutions across Europe. Explanation & relevance for Europe: As European governments rapidly adopt AI systems in public administration—including automated decision-making, risk assessment tools, digital public services, and data processing platforms—there is a growing need to ensure that these systems are transparent, explainable, and subject to effective oversight. Lack of clear transparency standards, insufficient auditing mechanisms, and inconsistent data protection safeguards can undermine trust, reduce fairness in public decision-making, and increase the risk of discrimination or misuse of personal data. This issue is part of a broader and more complex challenge: aligning AI deployment with European values, human rights, fundamental freedoms, and democratic accountability. Developing a shared European approach to transparency obligations, risk mitigation, algorithmic auditing, and cross-border cooperation would help ensure that public sector AI strengthens governance rather than creates new risks.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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	Grigor Nersisyan	Center for Public Finance and Personal Data Protection Monitoring, Education NGO	Civil society									The impact of AI-generated misinformation during crises and its influence on public trust and safety. Explanation: Across Europe, emergency communication is increasingly challenged by AI-generated misinformation, deepfakes, and manipulated crisis-related content. These tools can rapidly erode public trust, delay protective actions, and disrupt coordinated responses during natural disasters, conflicts, health emergencies or security incidents. This issue is connected to a wider problem of digital information integrity, crisis governance, and societal resilience. Addressing it requires stronger cooperation between governments, platforms, researchers and civil society to build reliable communication mechanisms, improve public awareness, and reduce cross-border risks stemming from malicious uses of AI.
7	Grigor Nersisyan	Center for Public Finance and Personal Data Protection Monitoring, Education NGO	Civil society									Strengthening Public Trust in AI-Driven Public Administration Through Transparency and Accountability Public administrations across Europe increasingly use AI systems for decision-making, risk assessment, and digital public services. While these tools improve efficiency, they also create concerns about transparency, fairness, explainability and the protection of individuals' rights. When algorithmic decisions appear opaque, public trust in institutions can decline. The issue is highly relevant for Europe because it affects all countries adopting AI in core public functions and is directly connected to the implementation of the EU AI Act, GDPR and emerging European interoperability standards. It raises important questions about human oversight, accountability and ensuring that AI-based public services remain aligned with fundamental rights. This topic is part of a broader challenge related to the complexity and opacity of algorithmic systems, the risk of discriminatory outcomes, uneven digital capacities across public authorities, and limited public awareness about how AI systems operate. Ensuring trustworthy and human-centric AI in public administration is essential for safeguarding democratic legitimacy and citizens' rights.
8	Wout de Natris-van der Borght	De Natris Consult	Private sector									With threats to democratic nations in Europe coming from all sides, it is time to redefine our relationship with the rest of the world. The digital realm is a huge part of this topic. What strategy is Europe developing or should it develop and what means does it need to deploy to become more ICT self-reliant? With the exception of access and literacy, this topic affects all categories but transcends them in direct impact and urgency.
9	Wout de Natris-van der Borght	DC Internet Standards Security and Safety Coalition	Civil society									With the investment into the development of quantum computers rising into the billions, the world comes ever closer to the scientist who has his or her "eureka moment". From that moment onwards some entity somewhere in the world will have computing power available that is currently imaginary only. To prevent this power from having devastating effects on all in the world, a transition towards the deployment of post-quantum cryptography is necessary. This is a task of enormous proportions. Just think of all the devices, servers, sensors, internet standards, OT and ICT that need a timely adaptation. Or, all the different stakeholders involved who have to prepare for this transition. And there is no time to lose. Where is Europe today? What are the current best practices? What initiatives are there? These are just examples of potential roads to explore under this topic.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

10	Zahiduzzaman Syeed	E-Farmers Bangladesh Ltd.	Private sector	■	■		■					Digital agricultural inclusion is becoming one of the most urgent policy challenges for Europe and its neighboring regions. As food systems face climate stress, AI-driven agriculture, remote sensing, and digital extension services are transforming how farmers access information, markets, finance, and climate-adaptive technologies. However, the digital divide between urban and rural communities continues to widen. The issue is highly relevant for Europe because agricultural supply chains are globally interconnected—food security, climate resilience, and technological standards increasingly depend on cross-border cooperation. Europe is also a major investor in digital agriculture and a key knowledge hub. Yet smallholder farmers across borders often lack access to digital skills, connectivity, responsible data governance, and interoperable digital tools. This issue sits within a broader cluster: rural digital transformation, digital literacy, fair data access, AI ethics in agriculture, cross-border standards, and inclusive digital innovation. Addressing it will help Europe strengthen resilience, sustainability, and international cooperation.
11	Babatunde Onabajo	ChurchMapped Limited	Private sector		■		■					Is "European sovereignty" the right approach to the adoption of technological solutions for Europe? Many European organisations and businesses rely on software produced by US companies such as Microsoft, Apple and OpenAI. However, there is a growing call among some that European countries should adopt a Europe-first approach when choosing a given vendor for a particular software solution. There are arguments both for and against this worldview, and it is hoped that this issue serves as a platform in which participants can discuss their views.
12	Clara Ruthardt	Bertelsmann Stiftung	Civil society		■	■		■				Social-media platforms have become critical infrastructures shaping how information flows, public debate unfolds, and democratic decision-making emerges. Yet today's digital public sphere is structurally fragile: it is highly centralized, dominated by a few non-European actors, and vulnerable to manipulation, opaque algorithms, and geopolitical influence. Mis- and disinformation are not isolated problems but symptoms of a weakened information ecosystem marked by monopolistic dependencies and attention-driven business models. Strengthening resilience requires moving beyond content-centric responses. Europe and global partners need to focus on interoperability, decentralised and open infrastructures, and accountable governance models that embed human rights, transparency, and democratic values. While EU instruments like the DSA and DMA set important standards, effective resilience demands consistent enforcement, global coordination, and support for open protocols and digital commons that reduce structural dependencies. This issue invites the EuroDIG community to explore how interoperable standards, open infrastructures, cross-border cooperation, and inclusive multistakeholder processes can reinforce digital sovereignty while safeguarding open, free, and secure information spaces worldwide.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

13	Michael Robinson	University of Vermont	Civil society			■						On page 35 of the EuroDIG report (Messages from Strasbourg 2, EuroDIG2025) the opening lines read: “It is important to find the right way to address child protection with age verification tools as these tools affect everybody, not just kids.” This phrasing is problematic. It (1) states a goal without defining it, (2) assumes a specific means (age verification) before public debate, and (3) uses vague language inappropriate for a document with legal consequences. Any proposal that restricts personal freedoms must cite the exact legal basis, define “child protection” and the specific harms to be addressed, and set measurable objectives. Policy-making should begin with problem definition and metrics: is the aim enforcement or prevention? If enforcement, list the statutes intended to be enforced, evidence that age verification is effective, and a cost-benefit analysis weighing law-enforcement gains against lost freedoms. If prevention, identify which crimes or harms are prevented, how age-ID would avoid false positives, and estimate the proportion of the population that are the real targets. Emotional appeals are not a substitute for legal and technical analysis. Before endorsing age-ID, Europe must publish clear legal citations, quantitative justifications, and rigorous analysis of risks to law-abiding citizens’ rights and privacy.
14	Torsten Krause	Stiftung Digitale Chancen	Civil society	■		■	■					From 2027 onwards all Member States of the European Union should issue the EUDI Wallet to their citizens. This wallet enables all citizens to identify themselves online in a secure manner and will therefore open up possibilities for e.g. personal authentication with public authorities, businesses and other. EuroDIG could provide a forum to inform all stakeholders about the current status of the development of the EUDI Wallet, perspectives of member states to realize the promise to issue this wallet in 2027 and also to discuss questions related on privacy, security and interoperability, as addressed in the Messages from Strasbourg 2025 (Main Topic 5) of the EuroDIG community and examine if the EUDI Wallet will be one solution to address the age verification dilemma.
15	Ioanna Skondra	Digital Democracy Foundation	Civil society	■		■			■			Across Europe, democracy is increasingly mediated through digital spaces. From local consultations and participatory budgeting to national policy dialogues and European-level initiatives, digital tools are reshaping how people participate in public life. Yet European citizens experience digital participation unevenly. Differences in digital literacy, accessibility, language, trust in institutions, and platform design mean that participation is often unequal, fragmented, or symbolic. This risks undermining a core European democratic principle: the right of everyone to participate meaningfully in public affairs. Digital Participatory Democracy focuses on how Europe can ensure that digital participation strengthens democracy, civil rights, and social cohesion, rather than deepening divides between those who can engage effectively and those who cannot. Grounded in European values, human rights standards, and multistakeholder governance traditions, this issue explores how digital democracy tools can be designed and governed to support inclusive participation across diverse European societies. Why This Issue Matters for Europe Now Europe faces interconnected democratic challenges: • Declining trust in democratic institutions across several European countries • Democratic backsliding and shrinking civic space in parts of the region • Unequal access to digital participation between urban and rural areas • Generational gaps in political participation, despite high digital engagement among youth

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

16	Iffat Rose Gill	The Code To Change	Civil society	■			■					For the last few years, we have been working on the issue of involving youth in designing the technologies that are impacting their lives. We are now starting debates in the Netherlands and Europe on the impact of Artificial Intelligence on the youth and the future of work. This also includes how the policies will be impacting the future of our next generation of leaders who will have to bear the consequences of policies we are making/supporting today.
17	Matthias Kettemann	Humboldt Institute for Internet and Society	Academia	■			■					Learning from Early Internet Governance for Frontier Technology Governance: In its formative decades, internet governance developed outside traditional state-centric regulatory frameworks. Instead, it relied heavily on standard-setting processes, (what we would now call) multi-stakeholder institutions, and forms of private rule-making, including technical standards bodies, industry consortia, and (later on) platform-based governance arrangements. Some of these mechanisms have enabled innovation, interoperability, and a degree of normative ordering in the absence of comprehensive public regulation. At the same time, they raised concerns that persist to this day regarding legitimacy, accountability, inclusiveness, and power asymmetries. As we now consider developing frameworks for governance of high and frontier technologies, including artificial intelligence, quantum computing, synthetic biology, and advanced semiconductors, similar dynamics are re-emerging. So what lessons can be draw? I would suggest pulling together lessons from early internet governance experiences for contemporary high-technology governance, especially in light of commitments in the WSIS+20 outcome document adopted in December 2025.
18	Lars Steffen	eco – Association of the Internet Industry / EuroISPA	Private sector			■				■	■	Encryption Under Pressure: Balancing Security, Privacy, and Law Enforcement in Europe: End-to-end encryption (E2EE) is a cornerstone of secure communications and data protection in the digital age. However, ongoing debates in the EU - particularly in the context of combating child sexual abuse material (CSAM) and other serious crimes - have reignited proposals to introduce mechanisms that could weaken or circumvent encryption. Key issues include: • Technical feasibility and risks of client-side scanning or backdoors. • Impact on fundamental rights, including privacy and freedom of expression. • Trust and security implications for businesses and consumers. • Legal and regulatory uncertainty: How dies weakening encryption align with GDPR, the ePrivacy Directive, and cybersecurity strategies? Questions to be addressed: • What are the current legislative and policy proposals in the EU regarding encryption? • Can law enforcement needs be reconciled with strong encryption? • What are the potential consequences for cybersecurity, innovation, and user trust? • Are there alternative approaches that respect rights and security? Relevance to EuroDIG: Encryption is essential for secure digital services, e-commerce, and democratic resilience. Weakening encryption could have far-reaching consequences for Europe's digital sovereignty and trust in online services. EuroDIG offers a multistakeholder platform to discuss these tensions and explore balanced solutions.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

19	Lars Steffen	eco – Association of the Internet Industry / EuroISPA	Private sector			■				■	■	E-Evidence Regulation: From Adoption to Operationalisation – Challenges and Solutions: The EU's E-Evidence Regulation, adopted to streamline cross-border access to electronic evidence in criminal investigations, is entering its implementation phase. While the regulation aims to improve efficiency and legal certainty, its operationalisation raises significant questions for service providers, law enforcement authorities, and judicial systems across Member States. Key issues include: • Technical and procedural readiness of service providers to handle European Production and Preservation Orders. • Legal fragmentation and interaction with national laws, GDPR, and fundamental rights. • Safeguards for due process and proportionality, especially in cross-border contexts. Questions to be addressed: • How prepared are stakeholders for the regulation's entry into force? • What operational/technical hurdles exist for providers and authorities? • How can transparency, accountability, and user rights be ensured? • What best practices and tools can support compliance and efficiency? Relevance to EuroDIG: The E-Evidence Regulation directly impacts the European digital ecosystem, shaping trust, security, and fundamental rights online. Its implementation will influence cross-border cooperation, data governance, and the responsibilities of internet service providers. EuroDIG provides a unique multistakeholder forum to discuss these issues and foster dialogue between all relevant stakeholders.
20	Torsten Krause	Stiftung Digitale Chancen	Civil society	■		■		■				Both the European Commission and the Member States consider the protection of children from harmful content, addictive design, data exploitation, sexual violence and algorithmic risks in social media to be an important priority. However, their approaches to achieving this appear to differ. In the summer of 2025, the European Commission released guidelines for a safe digital environment for children in line with Article 28 of the DSA. It's counting on providers to use the advice and recommendations to make their services more child-friendly. Regardless of this, many Member States are considering restrictive measures for young people's access to social media. They seem to trust neither the providers nor the Commission to enable the safe participation of children and young people in this way. Their opinion often plays no role in this. But how can we work together to create a safe internet for young people that takes children's rights into account and allows Europe to act in a unified manner?
21	Nenja Wolbers	Stiftung Digitale Chancen	Civil society	■								Europe's digital transition offers a strong opportunity to strengthen rural and peripheral communities by improving access to public services, social interaction, and local economic activity. In regions such as rural Southern Europe, Alpine areas, Northern Scandinavia, Eastern Europe, and island regions, inclusive digital solutions can help overcome geographic distance, demographic change, and limited service availability. This issue is part of a broader European challenge: ensuring that digitisation contributes to territorial cohesion and social resilience. Locally embedded, low-threshold digital platforms can connect citizens with local administrations, simplify administrative procedures, and integrate everyday services such as mobility information, healthcare coordination, local marketplaces, and community events into one accessible interface. Unlike global social media platforms, these solutions are designed to strengthen neighbourhood-level interaction and civic engagement. For Europe, the relevance lies in promoting people-centred digitisation that builds trust, encourages participation, and supports democratic resilience. Co-creation approaches involving citizens and local authorities from the outset are essential to ensure acceptance and long-term impact. Addressing this issue in a conference setting enables stakeholders to share experiences, identify transferable solutions, and discuss how inclusive digital platforms can support resilient economies and responsive public services across rural Europe.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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	Javid Alasgarli	Azerconnect Group	Technical community									People talk about digital security like it's just a tech problem, but honestly, it's a lot more personal than that. If your login is a complext to remember, if some website keeps asking you for way too much info, or if you have no clue where your data is actually going, you start to feel exposed. Unsafe, even. These little details such as things designers and engineers sometimes overlook and end up deciding how much of your private life leaks out and whether you trust these digital services at all. A lot of today's digital systems are confusing or disconnected. Some companies think grabbing even more data will solve things, but that usually just makes the mess bigger when things break. Plus, it gives more chances for your information to be misused. When you cannot figure out how a system works, you lose any real grip on your own data, and it's tough to push back or even ask questions. That's why building these systems is not just about code or hardware — it's about people. If you keep things simple, make the rules clear, and build privacy into the foundation, you protect people. You help them avoid unfair treatment, abuse, and you keep their trust. Europe has a good example at leading the way here, just by focusing on how these systems play out in real life. When security is straightforward and fair, when you can actually understand what's going on, people are way more likely to trust digital tools, and actually use them with confidence.
23	Sascha Nies	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH	Government									Strengthening Youth Participation in European Internet Governance Young people are increasingly affected by digital policy decisions, yet their participation in European and global internet governance processes often remains limited or symbolic. While interest among students and young professionals is high, access to policy spaces, informal networks, and practical experience remains uneven. As a result, youth participation often stops at observation rather than enabling meaningful contribution. Fellowships, mentoring, and youth engagement programmes aim to address this gap, but their long-term impact varies. A key challenge is moving beyond one-off participation toward sustained engagement, skills development, and pathways into policy-relevant roles within the multistakeholder ecosystem. We want to explore how youth participation in internet governance can be made more meaningful and effective. It will discuss the competencies young participants need, the role of institutions and stakeholders in mentoring and integration, and how existing initiatives across Europe can better align and learn from each other. Relevance to EuroDIG: Meaningful youth participation is essential for the legitimacy, continuity, and sustainability of the multistakeholder model. EuroDIG provides a unique platform to reflect on current practices, share lessons learned, and identify concrete steps to strengthen youth participation in European internet governance.
24	David Frautschy	Internet Society	Technical community									Efforts to block online content through the Domain Name System (DNS) or IP-based measures are increasingly used as policy shortcuts to address online harms—but they are blunt, ineffective, and often counter-productive. Such interventions do not remove harmful material; they merely distort the operation of the Internet's naming and routing infrastructure. Mandated blocking can be easily circumvented, risks over-blocking lawful content, fragments global name resolution, weakens DNS security (e.g. DNSSEC), and creates cross-border legal and operational conflicts. The Internet Society proposes a session to explore how content blocking affects the integrity of the Internet, share technical and policy perspectives from operators and governance bodies, and discuss alternative, source-focused and multistakeholder approaches that uphold the Internet's openness, resilience, and trustworthiness.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

25	Dorijn Boogaard	NL IGF	Other	■			■	■				Development of the IG ecosystem With the WSIS+20 outcome document recently adopted and the IGF's mandate made permanent, EuroDIG 2026 provides a timely opportunity to reflect on and further strengthen the European Internet Governance ecosystem. In a rapidly evolving geopolitical and technological context, EuroDIG 2026 offers an important platform to build on the ecosystem's strong multistakeholder foundations and to consider its future direction. Innovation & economic issues In the context of increasing geopolitical tensions and rapid technological change, Europe's innovation capacity and economic resilience are closely linked to questions of digital strategic autonomy. EuroDIG 2026 offers a valuable opportunity to examine how Internet Governance frameworks, standards and policy choices shape Europe's ability to innovate, remain competitive and reduce critical dependencies, while continuing to uphold fundamental rights and an open internet. Media & content EuroDIG 2026 offers an important opportunity to discuss how Europe can address online harms and illegal content, such as terrorism and radicalisation, while safeguarding democratic values through cooperation, dialogue and shared responsibility across stakeholders.
26	Eleftherios Chelioudakis	Homo Digitalis - NGI TALER (consortium)	Civil society			■	■				■	Europe is at a critical crossroads in shaping its future payment infrastructure. As the Digital Euro advances, fundamental questions arise about how digital payments should balance innovation, economic efficiency, technical resilience, and the protection of fundamental rights. The core issue is what kind of digital payment ecosystem Europe chooses to build. The Digital Euro promises efficiency and monetary sovereignty, but it also raises concerns regarding privacy, security, governance, and potential financial surveillance. Design choices made today will have long-term consequences for trust, inclusion, and democratic accountability. GNU Taler, the free software and privacy-preserving payment system, co-funded by the European Commission under the Next Generation Internet (NGI) TALER project, represents a unique opportunity for digital payments. It enables democratic control over the payment infrastructure itself, while its privacy-by-design architecture ensures that payers remain anonymous by default, while recipients are accountable, closely mirroring the properties of physical cash in the digital environment. This issue lies at the intersection of human rights & privacy (financial autonomy and freedom from surveillance), innovation & economic policy (open standards versus vendor lock-in, SME inclusion), and technical & operational challenges (auditability, security, scalability).
27	Isabella Ridout	Google	Private sector	■								Information literacy is crucial for democracies in the digital age. Having the skills and information to assess the trustworthiness of content encountered online is a key component of information literacy. In light of recent developments in generative AI, many suggest that information about the way content was created (by AI or otherwise) can be a proxy for assessing trust. However, "Is this AI-generated?" is not equivalent to "Is this trustworthy?" This issue is critical to the European digital landscape as the region enters the implementation phase of the EU AI Act. European stakeholders must now determine how legal mandates for labeling synthetic content translate into meaningful user understanding rather than mere technical compliance. Furthermore, protecting the integrity of the information ecosystem is a primary pillar of the European Democracy Action Plan. The development of robust provenance frameworks, effective contextual tools, and multi-stakeholder capacity building is essential to safeguarding public discourse. We hope to discuss novel approaches to information literacy that focus on making contextual and provenance information about content available to users. This includes tools that provide assertive content provenance information, such as C2PA and SynthID content watermarking standards, as well as AI tools that help provide more context and assess informational claims.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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	Barbara Crepaldi	Eumans	Civil society		■	■			■			AI AND DEMOCRACY Today AI is in the hands of a few and that's a huge risk for democracy. That is why the EU should implement a AI-powered civic eco-system that serves the common good, promoting the public and open development of AI models under democratic control, with an aim to: Strengthening democratic participation, Ensuring open access to scientific information, Promoting open-source solutions, Protecting individual rights and democratic values The goal should be that of creating an environment where citizens can be more actively involved in public decisions, while AI systems are developed to serve the collective interest, not the interest of a few
29	Oona Kurppa	Generation Equality -youths	Civil society			■				■	■	Online violence is a threat to democracy and human rights across borders. Online violence disproportionately affects women, as patriarchal social structures sustain the continuum of violence, also in digital spaces. Harm is often inflicted across national boundaries and amplified by global social media and gaming platforms. Technology companies and platform owners play a critical role in prevention and response to online violence. At the same time, online violence frequently overlaps with offline violence. Perpetrators are often known to the victim, which makes effective national legislation and well-resourced local authorities essential. In many European countries, the specific dynamics of online violence are not yet fully recognised in law. The absence of harmonised measures and shared standards leads to fragmented responses, uneven enforcement, and inconsistent support for victims. Globally, children, youths and other vulnerable groups are more likely to be targets of online violence. According to the WHO (2025) one in three internet users globally is a child. Some 80% of children in 25 countries report feeling in danger of sexual abuse or exploitation online (The UN, 2025). While the EU has taken steps to address online violence, current measures remain insufficient. Europe has an opportunity to lead in developing rights-based and future-proof digital governance. EuroDIG provides a crucial platform for advancing this issue toward coordinated and concrete European solutions.
30	Alena Muravska	RIPE NCC	Technical community								■	As discussions continue on the future of Internet governance beyond WSIS+20, a key challenge that needs closer examination is how global commitments to an open, secure and inclusive Internet are put into practice. Open and interoperable Internet standards are essential to achieving sustainable development, supporting trustworthy digital public infrastructure, and enabling social and economic participation online. However, while these standards are developed through open and consensus-based processes, their uptake and correct deployment remain inconsistent. This disconnect between availability and implementation creates risks for interoperability, security, and long-term resilience of the Internet. The issue therefore lies not in the lack of standards, but in how they are adopted, implemented, and maintained across different contexts. Governments, the technical community, the private sector, and civil society each play distinct but interdependent roles in this process. Policy tools such as procurement rules, regulatory baselines, and national transition plans can encourage adoption, but they are most effective when informed by technical expertise and supported by collaborative testing, monitoring, and knowledge-sharing. By linking WSIS follow-up, the 2030 Agenda, open Internet standards, and multistakeholder cooperation, this issue highlights the need to better understand and strengthen practical, cooperative approaches that turn shared principles into reliable, interoperable, and accessible digital infrastructure.
31	Marc Kölliker	Etuna St Johann (School for Special Needs)	Civil society	■		■					■	Education Technology brings Big Chancen to special needs education. National Governance does not Set standards for Special needs education, mostly there is no explicite finance for it. As a Special needs teacher working with Ed Tech with children with Social disabimities I See a huge benefit of Ed Tech for my Students .

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

32	Niklas Schmidt	Federal Office for the Enforcement of Childrens's Rights in Digital Services (KidD)	Government									Enforcing children's rights in the digital world requires effective international cooperation between the relevant stakeholders. Only on this basis can the key provisions of the Digital Services Act be effectively enforced. This cooperation is also a prerequisite for the widespread introduction of age verification systems at the international level, which are central to the protection of children and young people in the media. These systems provide the basis for structural precautionary measures on online platforms ("safety by design" and "safety by default") to be effective. Only when the age or age group of users is known can protective mechanisms be adapted and take effect. Compliance with minimum age limits is only one – albeit central – function of these systems. Another example of a function of these systems is to restrict communication between certain age groups in order to prevent dangerous phenomena such as cybergrooming. When designing these age verification systems, it must be ensured that a data-minimizing design is chosen that does not grant the platforms access to personal data – such as dates of birth – of their young users. Enforcing the introduction of such age verification systems on central online and social media platforms is a key task of international cooperation for the enforcement of children's rights.
33	Murillo Salvador	Swiss Youth IGF	Civil society									We propose to explore how social media influencers can become active participants in internet governance: not as outreach targets, but as legitimate stakeholders with unique expertise and direct community connections. Their experience at the frontlines of the digital economy could further enhance the multistakeholder model. Influencers are among the most affected actors when it comes to platform governance, algorithmic changes, content moderation, and digital rights. Their professional existence depends on policy decisions made in forums from which they are absent. Influencers are increasingly embedded in political communication: an European Commission 2025 study shows 74% of young Europeans follow influencers, while a German 2024 study reveals that 59% of political influencer content blurs the line between opinion and information. Meanwhile, grassroots mobilization by fora such as EuroDiG faces two problems: limited online reach relative to the general public; and volunteer-driven engagement concentrated around yearly events, missing a chance for sustained community building by digital natives themselves. Rather than asking how IGFs can generate more online engagement, we ask: how can the IGFs adapt to become relevant for those who already command grassroots followings? For example: • What is distinct about this "digital native stakeholder" group? • What mutual benefits exist between the IGFs and influencers? • What pathways exist for converting influencers' social capital into policy participation?
34	Arden Haselmann	Google	Private sector									2026 is slated to be the year of AI agents: a new generation of artificial intelligence where systems are capable of independent action and decision-making. As these systems begin to operate autonomously they raise fundamental questions for the global landscape of internet governance. We propose a deep dive into the critical considerations surrounding the development and deployment of agentic AI. Central to this discussion are questions like What are the foundational principles that should be used to guide the development and deployment of agentic AI? How do we ensure these systems align with human values and societal norms? How do we address concerns around user safety and personification of AI? How do we mitigate the risks of misuse and malicious actors? What novel risks or challenges are raised by agentic AI? How should companies govern what data agents should have access to? How do we manage the trade-off between privacy and effectiveness? How can we balance agentic autonomy with rigorous oversight and end-user control? Through cross-community engagement, a discussion around this topic would help to better establish a foundation for responsible innovation in the age of agentic AI and think through how to embed user-centricity in the building and deploying of agentic products.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

35	Grit Marti Lange	Netzforma* e.V.	Civil society			■		■		■		Antifeminist Online Hate as a Democratic Threat Antifeminist online hate has become a central driver of digital violence and democratic exclusion. Rather than representing a marginal backlash, contemporary antifeminism functions as a widely normalised form of hostility that is deeply entangled with right-wing and anti-democratic ideologies. Women, feminists, and LGBTQIA+ persons -- particularly those who are politically visible -- are disproportionately targeted by harassment, intimidation, and coordinated hate campaigns. Research and civil society monitoring that antifeminist digital violence produces clear silencing effects: self-censorship, withdrawal from public debate, and reduced political participation. These dynamics undermine democratic pluralism by shaping who can safely speak and remain visible in digital public spaces. At the same time, antifeminist hate cannot be understood as merely discursive harm. Antifeminist worldviews have been identified as contributing factors in right-wing radicalisation processes and extremist violence, including attacks such as Christchurch and Halle. Digital platforms play a crucial role in this continuum by amplifying polarising content and embedding antifeminist narratives into everyday online environments. This issue invites discussion forms of digital violence (e.g. antifeminism) with structural democratic consequences.
36	Grit Lange	Netzforma*	Civil society			■		■		■		Digital Violence and the Limits of the DSA's Transparency Framework The EU Digital Services Act (DSA) represents a landmark achievement in platform regulation and a crucial step toward protecting fundamental rights and democratic participation in digital spaces. At the same time, its effectiveness depends heavily on transparency obligations, risk assessments, and platform self-reporting. This raises practical questions about what forms of harm become visible and actionable -- and which remain insufficiently addressed. In practice, transparency requirements have so far been implemented unevenly by platforms. Existing reports are often difficult to compare, lack contextual depth, and provide limited insight into how risks are identified, mitigated, or prioritised, particularly from the perspective of affected communities. Gender-based digital violence illustrates these challenges particularly clearly. Algorithmic amplification of misogynistic and hostile content, engagement-driven recommendation systems, and platform business models that reward polarisation are only partially reflected in current risk assessments. Moreover, reporting and redress mechanisms frequently remain opaque, fragmented, or inaccessible, limiting their usefulness for those exposed to online harassment and intimidation. This issue proposes a discussion not aimed at questioning the necessity of the DSA, but at strengthening its implementation.
37	Grit Lange	Netzforma* e.V.	Civil society	■		■				■		The Digital Services Act (DSA) is a central pillar of European digital governance and a key instrument for protecting democratic participation, fundamental rights, and safer online environments. At the same time, it is increasingly under political pressure -- from industry lobbying to direct attacks by US political actors framing it as "foreign censorship." These debates are not abstract. Civil society organisations and political actors working on platform accountability and digital violence are already facing tangible consequences, including political intimidation, as recently demonstrated by the German NGO HateAid. Weakening or abandoning the DSA would therefore have direct implications for democratic resilience. Regulatory frameworks that protect digital public spaces must not become bargaining chips in trade disputes or geopolitical negotiations, e.g. in exchange for lower tariffs. Digital sovereignty should be understood not only as control over infrastructure, but as the capacity to defend democratic rules for digital environments. This includes maintaining independent regulatory standards under external political pressure. The DSA plays a crucial role in addressing platform power and in countering democratic erosion. This issue calls for a discussion on why defending the DSA is essential for democratic self-determination and how Europe can safeguard its regulatory achievements in an increasingly contested geopolitical environment.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

38	Maciej Gron	NASK	Technical community									Trust and Safety - designing child-centered online protection is a strategic policy priority for the EU at the intersection of digital governance, fundamental rights and public trust. The accelerating evolution of online services requires coherent Trust & Safety frameworks that translate EU values into enforceable and effective protections for children, while safeguarding freedom of expression and privacy. A critical policy challenge remains addressing hate speech, online violence and the spread of CSAM, where fragmented responsibilities, cross-border enforcement and evidentiary constraints continue to test regulatory effectiveness. Instruments such as the Digital Services Act, alongside forthcoming EU initiatives, significantly expand platform obligations, yet their success depends on consistent implementation, institutional coordination and a clearly articulated child-centered policy approach. Digital education must be embedded as a complementary policy tool, strengthening prevention, resilience and informed participation. Empowering children through age-appropriate education, while equipping parents, educators and professionals with the necessary competencies, reinforces Trust & Safety governance beyond compliance. By integrating regulation, platform accountability and digital education, the EU can enhance policy coherence, reinforce societal trust in digital services and ensure that child protection remains a central pillar of Europe's digital policy agenda.
39	Kathrin Morasch	LFK- Media Authority of Baden-Württemberg	Other									"Hate Speech, DSA Enforcement and Platform Responsibility: Regulation, Backlash and the Future of Digital Rights" Recent developments around HateAid illustrate the growing tensions surrounding digital regulation. The US government has imposed entry bans on HateAid's managing directors and other European actors, arguing they pressured US platforms into censorship. We see this as retaliation against those supporting the enforcement of the DSA and the removal of illegal online content. At the same time, political debates increasingly focus on restricting social media access for young people as a response to toxic online environments. But why are platforms restricted for specific groups instead of being made safer and more accountable for everyone? Hate speech, antisemitism and misogyny are daily realities online, affecting all users. The DSA was designed to address these phenomena through clear obligations, transparency and enforcement, not through blanket bans that risk shifting responsibility away from platforms. This session can explores how the DSA can be enforced consistently and credibly, particularly in the area of hate speech an protection of minors. What does it mean when individuals and organizations tasked with implementing EU law face political backlash or even entry bans? Does this affect other Trusted Flaggers and actors such as media authorities as well? And where does this leave us if those simply applying existing legal frameworks are treated as threats?
40	Charalampos Kyritsis	EURid Youth Committee	Other									As Europe navigates an increasingly fragmented geopolitical landscape, the concept of "Digital Sovereignty" is becoming an increasingly relevant issue. Silicon, Networking and DNS are only some of the various layers of this issue which should be explored in more depth. Semiconductors: The global chip shortage exposed the fragility of supply chains dependent on Asia and the US. While the European Chips Act is a vital first step, Europe must accelerate its transition from research excellence to industrial capacity. Space: As ground networks face threats from cyberattacks and physical sabotage, space has become the new critical domain for resilience. The deployment of the EU's IRIS constellation is essential, but it must be more than just a government backup. From 5G to 6G: In order to transision from 5G to 6G we need to integrate the terrestrial and non-terrestrial networks. Establishing sovereign manufacturing and deployment of satellites is necessary for sovern telecom infrastructure. European DNS: Ensuring DNS resolution occurs on European-controlled servers is vital for safeguarding citizen data, cybersecurity resilience, and reducing reliance on foreign operators. Sovereign Cloud: The vast majority of Europe's data resides on server technology and cloud infrastructure owned by non-EU hyperscalers. This creates unacceptable risks regarding data residency and dependency. A sovereign European Internet requires investment in data center infrastructure and open-source hardware.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

41	Pascal Schneiders	Johannes Gutenberg University of Mainz	Academia	■			■	■				Very large online platforms and AI systems are bringing about a fundamental economic, epistemic, and cultural transformation of the information ecosystem. For example, 1) the largely uncompensated use of journalistic content as input for training AI systems, 2) the barely traceable throughput processes and 3) the error-prone quality of the AI output, as well as the declining visibility and relevance of journalistic sources pose challenges not only for the business model of news media, but also for the information and opinion-forming processes of citizens. This issue invites the EuroDIG community to discuss which (human and technological) actors can and should provide trustworthy, socially relevant, impartial information in the future and how the sustainable production and visibility of diverse, trustworthy information can be ensured.
42	Sara Pane	Sapienza University of Rome	Academia						■			AI undoubtedly represents the latest frontier of the digital transformation. Its generative and conversational integration in public sector's service delivery has revolutionized the interactions between institutions and citizens. To date, there's a growing interest in AI as a medium to encourage more inclusive citizen engagement practices. While this has the potential to revitalize democracies at a moment where polarization is driving fragmentation and growing skepticism, it also poses challenges that need to be critically addressed. Agency, sensitive data treatment and regulation as well as human oversight amongst all. For this reason, it is necessary to encourage an active exchange on this timely topic: how AI can be used to promote active participation whilst ensuring trustworthiness of AI systems. This calls into question the very core themes of anticipatory governance and foresight that need to be considered in the wider discussion about civic AI - which is somewhat limited in the current scenario.
43	André Melancia	Technical Community	Technical community			■				■	■	The last few years saw an increase in awareness for Human Rights issues (in multiple fronts). So called "democracies" have used the Internet, AI and protesters' footprints online to profile and persecute them. The complete loss of Democracy and Rule of Law in the USA, the ongoing arrests of thousands peaceful protesters in the UK, Germany and other EU countries, backed by these "Big Brother" companies, should worry anyone who strives for Human Rights, Freedom and the Rule of Law. Amongst other questions, what can we do to enforce proper privacy and respect of the law in the EU?
44	André Melancia	Technical Community	Technical community							■	■	Given the growing number of online scams (phishing emails, scam calls, calls to harvest voice and amongst others use the "I'm your son" scam, spoofing phone numbers, spoofing and stealing IP addresses and dormant AS ranges. What can be done to minimise these attacks? Some technologies exist, such as for email and DNS (SPF, DKIM, DMARC, DNSSEC, DoH, etc.), for website validation (previous plus HTTPS/TLS, PKI CAs/Certs, etc.) for internet routing (RPKI, IRR, BGPsec and other techniques), for traditional phone networks (where not much is validated, as anything is easily spoofed, historically unchanged for the last 50 years), as well as other easily compromisable communication channels. Technology already exists to mitigate >90% of these incidents. Why is it not used (or "enforced"), and many other obvious questions?
45	André Melancia	Technical Community	Technical community							■	■	Is AI the solution to all our problems? Nobody can contest that AI (Generative AI as well as "traditional" Machine Learning) has been incredibly useful in the last few years, finding new cures for viruses, early detection of cancer and other illnesses, and more. On the flip side, AI consumes far more resources than traditional computing (e.g. electricity, AC, generates excessive heat into the atmosphere, requires water sources depleting nearby homes of their supply, etc.). Is that all really needed? Many marketing-driven companies force AI (e.g. chatbots) on people, when a traditional website would be easier to navigate, or simply replace humans with a poorer chatbot/phonebot experience. Where do we draw the line of what is useful and what is abusive and counterproductive?

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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	Peter Koch	DENIC eG	Technical community									The Internet's success is based on open standards with interoperability and security as key criteria. Another important aspect is the voluntary adoption of standards, which may lead to competition or co-existence of approaches to a certain network interoperability task. What does that mean for the deployment of complex, maybe even not backwards compatible new protocols at the very core of the network? What are the economics of change (read: "first mover disadvantage")? What lessons does recent history serve and how can multi stakeholder processes help?
47	Maarten Bottermann	GNKS Consult BV	Other									Internet standards: GFCE released its new Handbook on internet standards; the European Commission is in the process of setting up a “Multistakeholder Advisory Body” on Internet standards … all good stuff to talk about: what, why and how
48	Maarten Bottermann	GNKS Consult BV	Other									IoT: remains relevant … even more so, and lets look specifically at the impact of AI and PQC
49	Maarten Bottermann	GNKS Consult BV	Other									Threat intelligence and the need to better predict attacks and identify vulnerabilities
50	Karen Mulberry	IEEE	Technical community									Connecting the Digital Product Passport (DPP) to Governance, Standards and Interoperability The European Digital Product Passport (DPP) and Critical Raw Materials Act are the components of Europe's move towards a circular, sustainable economy in support of the EU Green Deal. DPP creates a new layer of digital governance, and its success is dependent on its governance design with associated standards development and alignment. The issue then is in defining the governance structure with the complexity that needs to be addressed and establishing the standards that are needed to support the governance requirements.
51	Karen Mulberry	IEEE	Technical community									The Energy-Water Nexus – Environmental impacts of emerging technology The EUs energy and water systems are interdependent and facing new environmental impacts from the needs of emerging technology. There is a need to holistically address the energy-water nexus to reduce Europe’s vulnerabilities and address systemic risks.
52	Karen Mulberry	IEEE	Technical community									Children in the Digital Environment Children are the most active and vulnerable participants in the digital environment, failure to address children’s rights and needs risks increased harm, inequality, and erosion of trust in digital systems. Digital technologies shape how children learn, socialize, access information and engage with society, ensuring that children can safely participate online is essential to a child-centered digital strategy to strengthen Europe’s values based governance model.
53	Peter Koch	DENIC eG	Technical community									With the results of the WSIS+20 process still being digested, we should should engage in a critical reflection on the role of the IGF and NRIs, especially in the multilateral vs. multistakeholder setting. What are the odds of continued 'industry self regulation' vs. multistakeholder laundering?
Additional proposals												

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

54	Oana Girlescu	HELP Programme of the Council of Europe	Intergovernmental organisation	■		■						Legal Professionals Navigating Hybrid/E-learning Choices The rapid development and availability of e-learning platforms and digital resources for legal professionals offer tremendous opportunities for ongoing education. Technology is transforming the way law and jurisprudence are accessed, learned, and applied. However, the abundance of choices can make it difficult for judges, prosecutors, and lawyers to select appropriate materials that reliably promote core values such as human rights. Furthermore, levels of digital literacy vary amongst these professionals, and the need to address the complexities of contemporary legal issues is often overwhelming. A number of key issues merit discussion: How to foster greater digital literacy among legal professionals to maximise the benefits of e-learning. Ways to identify, curate, and promote high-quality digital learning materials focused on human rights. The role of technology in both facilitating legal work and posing new human rights challenges, and how education can address these issues. Strategies for multi-actor collaboration to empower legal professionals with relevant, accessible, and actionable human rights knowledge. We can jointly explore best practices for curating effective e-learning content, strategies to improve digital literacy among legal professionals, peer and blended learning approaches, and models for collaboration. Whilst these issues are clearly relevant for the general public, they become even more pressing for the legal sector, given their impact on how our justice systems operate.
55	Daniel Schmidt	Council of Europe	Intergovernmental organisation	■		■	■					Generative artificial intelligence and justice: The good, the bad and the ugly. The use of generative artificial intelligence (AI) by legal professionals is growing, whether for summary generation, text correction, drafting legal documents based on case law, or interacting with litigants (e.g. explaining sentences to clients). Many countries are facilitating the use of generative AI tools in public administration and courts. While the implementation of AI in judicial systems has the potential to increase efficiency, it also raises questions that could threaten public confidence in the judicial system. These include a lack of transparency and explainability, the erosion of human judgement and empathy, and the risk of discrimination. There are also concerns about data security and integrity, democratic legitimacy, and accountability. Another significant challenge is the radical transformation of the legal profession, with fears that job losses could prevent the needs of litigants from being met. Related sessions should address two main questions: Firstly, how can (generative) AI be deployed productively to improve the law in line with human rights and the rule of law? Secondly, how can we ensure that the justice system remains a fair and trusted conflict resolution mechanism that supports social cohesion and societal prosperity?
56	Evangelia Vasalou	Council of Europe	Intergovernmental organisation					■				Media Coverage of Elections: Shaping Public Opinion in the Digital Age Elections shape democratic discourse, serving as a mechanism for political choice through which public opinion is formed, contested, and expressed. In the digital age, public opinion is influenced by algorithms, platform/AI-driven content, and user-generated media, creating opportunities for pluralism while also raising risks such as disinformation and polarisation. Against this backdrop, media coverage should be guided by democratic values supporting ethical journalism. Council of Europe standards remain a vital safeguard, ensuring that media continue to fulfil their democratic function despite evolving technological challenges. This approach aligns with the Council of Europe's vision for democratic resilience, reflected in the New Democratic Pact for Europe, which highlights the need to strengthen democratic participation and media freedom. Recent Council of Europe instruments—PACE Resolution 2254 (2019) and Resolution 2326 (2020) —build upon existing standards, addressing the risks of the digital information ecosystem. This session will foster dialogue among policymakers, media regulators, journalists, civil society, and platforms. It will examine the impact of digital media on elections and public opinion. Participants will discuss best practices for ethical, impartial, and transparent media coverage, exploring also regulatory frameworks as well as other means of strengthening democratic resilience.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

57	Charlotte Gilmartin	Council of Europe	Intergovernmental organisation	■		■			■			Emerging technologies are profoundly shaping European societies. They can strengthen gender equality by improving access, participation, and empowerment for women and girls. At the same time, technology also creates and amplifies structural risks for women and girls, including new forms of violence, discrimination and exclusion in online and offline spaces. Technology-facilitated violence against women and girls causes serious and lasting harm, reinforces gender inequality and leads to silencing women and girls, limiting their participation in public life and democratic processes. Artificial intelligence systems may reproduce or exacerbate gender-based discrimination through biased data, design choices or lack of transparency and accountability. The work of the Council of Europe's monitoring body on violence against women (GREVIO) is revealing a growing prevalence of online and technology-facilitated violence against women in Europe, including through the use of AI technologies. Effectively addressing these challenges calls for coordinated efforts across governments, civil society, and the technology sector. EuroDIG offers a timely multi-stakeholder platform to examine the impact of technology on gender equality and to explore how it can be governed in a way that protects rights, prevents harm, and advances gender equality across Europe.
58	Menno Ettema	Council of Europe	Intergovernmental organisation	■		■				■		AI is increasingly permeating every aspect of our daily lives, presenting significant challenges to the protection of fundamental rights. Algorithmic discrimination emerges as a particularly pressing concern. Research has demonstrated that algorithmic bias not only reflects but also exacerbates existing social inequalities. Building on new studies, it is proposed to reflects on how the EU AI Act and the Council of Europe Framework Convention on artificial intelligence and human rights, democracy and the rule of law strengthening protections against algorithmic discrimination, assesses the lacunae, and reflect on role of national human-rights structures, national authorities, civil society and groups at risk of discrimination can identify and mitigate the risks.
59	Cesare Pitea	Council of Europe	Intergovernmental organisation	■				■			■	Media Pluralism in the Age of AI-Driven Information Environments Media pluralism is essential to democratic societies. Today, the diversity and quality of content people see are heavily influenced by the algorithms of recommender systems and AI-driven content generators. As a few major platforms shape access to information, several pressing questions arise: • How can we define and protect media pluralism in environments governed by algorithms? • Can media pluralism be separated from reliability and trustworthiness? • Should assessments of systemic risk address pluralism, and how can this be measured? • What measures could restore user agency, allowing individuals more control over their information feeds? • Could "pluralism of recommender systems," such as user choice among third-party recommendation tools, foster more diverse media content? • As large language models (LLMs) become key sources of information, how can media pluralism be built into their development and use? This discussion will convene policymakers, technologists, and civil society to share perspectives and consider practical steps to support pluralism in digital information systems. Collaborative dialogue can help clarify the risks and opportunities posed by AI, shaping policies and technologies that promote open, diverse, and trustworthy information environments.
60	Diana Ceausu	Council of Europe	Intergovernmental organisation									Financial Sextortion and the Protection of Minors in Digital Europe The rapid growth and increasing severity of financial sextortion is highly relevant for Europe as a cross-border cybercrime that directly threatens the safety, mental health, and digital rights of children and adolescents. With sextortion reports rising at an unprecedented pace worldwide, most involving financial demands and predominantly affecting boys aged 14–17, the phenomenon targets a key demographic within Europe's highly connected youth population. The involvement of organised international criminal groups operating mainly from outside the EU, highlights the need for strong European-level cooperation in law enforcement, judicial action, and partnerships with third countries. The financial dimension—where victims make payments, and they continue to be extorted even after paying—also affects Europe's digital payment ecosystems and anti-money-laundering efforts. Most urgently, with a consistent number of teen suicides or cases referencing self-harm linked globally to sextortion, financial sextortion constitutes a serious child protection and public health concern, making it a critical issue for Europe's policies on online safety, mental health, and the protection of minors in digital spaces.

List of proposals for EuroDIG 2026 *(updated as of 30 February 2026)*

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

61	Octavian Sofransky	Council of Europe	Intergovernmental organisation									Digital businesses support for integrity, accountability and the rule of law Democratic standards, judicial independence and respect for international law are not only normative commitments but core economic infrastructure, essential for stability, fair competition and sustainable growth. Where legal certainty erodes and arbitrariness prevails, investment confidence declines, risks increase and prosperity becomes fragmented; corruption and attacks on independent institutions further distort markets and undermine both citizen trust and investor confidence. Digital businesses engagement for strengthening integrity, accountability and the rule of law should therefore be treated as a strategic opportunity, supporting governments and regulators' efforts. Artificial intelligence as both a challenge and an opportunity for democratic economies, requires enforceable, human-rights-based governance frameworks that ensure transparency, accountability and meaningful human oversight. Such frameworks provide legal certainty for innovation and investment while safeguarding democratic values, positioning trust-based governance as a competitive advantage in an increasingly AI-driven global economy.
62	Biljana Nikolic	Council of Europe	Intergovernmental organisation									Workshop on Product Tracking for Sustainable and Human Rights–Compliant Business Practices This session will explore how various instruments, including digital tools can enable transparent, product-level tracking to support sustainability goals while maintaining, and possibly even boosting competitiveness. It will examine how product tracking can help businesses measure environmental and social impacts across supply chains, improve resource efficiency and meet regulatory requirements without creating undue burdens. Crucially, the discussion will centre on designing product tracking methods/tools in ways that are compliant with human rights, ensuring data protection, non-discrimination, fair labour practices and meaningful accountability for all stakeholders involved.
63	Albina Ovcearenco	Council of Europe	Intergovernmental organisation									AI Regulatory Sandboxes: Advancing Human-Rights-Based Innovation As artificial intelligence systems increasingly shape societies, regulatory sandboxes are emerging as a practical governance tool to support innovation while safeguarding human rights, democracy and the rule of law. This session explores how AI sandboxes can operationalise human-rights-based approaches to AI throughout the system lifecycle, from design and testing to deployment. Drawing on concrete sandbox experiences from Ukraine, Switzerland and Spain, the session will examine how public authorities and innovators use controlled testing environments to identify and mitigate risks, clarify regulatory expectations, and embed safeguards at an early stage. The discussion will highlight how sandboxes can strengthen accountability, transparency and institutional learning, while supporting responsible experimentation. The session will situate sandbox practices within the broader European and international governance landscape, including the Council of Europe's Framework Convention on Artificial Intelligence, and briefly reflect on interactions with other regulatory initiatives. Particular attention will be paid to how sandbox insights can inform policy development, improve risk assessment practices, and foster coherence across jurisdictions without undermining innovation. By bringing together regulators, practitioners and other stakeholders, the session aims to identify good practices and shared lessons on how AI sandboxes can become durable instruments for trustworthy, human-centred AI governance.