

List of proposals for EuroDIG 2024 (as of 1 January 2024)



- 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

ID	Submitted by	Affiliation	Stakeholder Group	Categories the proposal is related to								Suggested issue	
				Access & literacy	Development of IG ecosystem	Human rights & privacy	Innovation & economic issues	Media & content	Other category	Security & crime	Technical & operational issues		
1	Miguel Vidal	Deutsche Telekom	Private sector		■		■					■	Who owns the Internet? A lot has changed on the Internet in the last ten years: It's not just applications and business models that have emerged or evolved. Less obvious, because hardly recognizable to many users, the architecture of the Internet has also changed fundamentally. The long-cherished model of a decentralized Internet infrastructure, in which thousands of different networks are involved in transporting the world's data traffic, is losing importance. Today, the lion's share of traffic flows through proprietary backbone networks and content delivery networks owned by large Internet companies and hyperscalers. This drastic shift in traffic from the public Internet to private networks has fundamentally changed the Internet ecosystem and led to a significant concentration of market power in the engine room of the Internet. The growing disparity between the public Internet and large private networks calls for a reassessment of existing policies and regulatory frameworks in Europe and beyond. Policymakers might choose strategies based on industrial policy goals to counter trends of global private networks emerging as dominating platforms. Such policies might also focus on other aspects such as cloud and data sovereignty, data governance, and data sharing.
2	Amali De Silva-Mitchell	IGF DC DDHT	Other	■		■	■						What is the status of the European inter-country medical records system development with respect to ease of data sharing, accessibility, privacy, research collaboration etc.? What are the emerging issues and how are accommodations for minority groups with language, accessibility or income limitations being managed for equal quality access?
3	Amali De Silva-Mitchell	IGF Dynamic Coalition on Data Driven Health Technologies	Other	■	■	■							What are the new developments in Virtual Reality, Augmented Reality and other emerging and advanced features of human to computer interaction assisting the ecosystem of ehealth, health research and health education? What issues must be resolved to enable the use of these advanced features? Are there any risks associated with using these features? How can equality of access for All UN SDG 3 Health and Wellness for All e.g. accessibility, be enabled using these features?
4	Babatunde Onabajo	ChurchMapped Limited	Private sector				■						Large language models (LLMs) have become an increasing part of artificial intelligent tools such as ChatGPT. The development has been significantly disruptive to sectors such as education and law, forcing key stakeholders to ask questions about the opportunities and dangers the developments pose to their respective industries. This issue for EuroDIG 2024 relates to whether LLMs, together with comparable technologies in the field of image generation, are compatible with copyright law in Europe? Will such tools increase, have no effect or decrease innovation in the creative sector?
5	Riccardo Nanni	Fondazione Bruno Kessler	Technical community		■		■					■	Dataspaces The 2020 EU Data Strategy envisages the creation of EU-wide dataspace covering key policy themes. The dataspace are to allow public and private actor to harness third-party data within the rules set by GDPR, the Data Governance Act and the forthcoming Data Act (among other legislations) to provide citizens with services and to make policies. However, the implementation of such dataspace is lagging and the EU, despite its regulatory effort, remains uncompetitive compared to countries like China or the US due to a lack of a world-leading domestic industry. Furthermore, legal clarity is lacking as the data-related legislation is still emerging. I believe discussing this topic is of timely relevance to foster the creation of a data governance ecosystem that supports decisionmaking based on data.

List of proposals for EuroDIG 2024 (as of 1 January 2024)



- 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

11	Liljana Pecova Ilieska	IMPETUS	Civil society		■											<p>Cyber Pandemic Preparedness: Strengthening Europe's Digital Defenses</p> <p>Description: This topic focuses on the need for Europe to enhance its cybersecurity measures and preparedness in the face of evolving cyber threats. It explores strategies, policies, and collaborations to protect critical infrastructure, organizations, and individuals from cyberattacks. The term "cyber pandemic" refers to a widespread and disruptive cyberattack or series of attacks that could have severe consequences, much like a biological pandemic.</p> <p>From Smart Cities to Wise Communities: Building Sustainable Urban Tech Ecosystems</p> <p>Description: This topic examines the concept of smart cities and how technology can be leveraged to create more sustainable and livable urban environments. It goes beyond the technical aspects and delves into the social and environmental dimensions, emphasizing inclusivity, sustainability, and community engagement in the development of urban tech ecosystems.</p> <p>Web3 and Decentralized Web: The Future of Digital Ownership</p> <p>Description: Web3 refers to the third generation of the internet, characterized by decentralized technologies, blockchain, and the idea of giving users more control over their digital presence and assets. This topic explores the potential of Web3 and the decentralized web to reshape how individuals own and interact with digital assets, data, and online platforms. It delves into concepts like decentralized identities, digital wallets, and decentralized applications (dApps).</p>
12	Liljana Pecova Ilieska	IMPETUS	Civil society					■								<p>Secure Digital Identities: Unlocking Trust in Online Transactions</p> <p>Description: This topic revolves around the importance of secure digital identities in the digital age. It discusses the challenges associated with online identity verification, data privacy, and fraud prevention. The focus is on exploring solutions and best practices for establishing and managing secure digital identities that can be used to build trust in online transactions, whether in e-commerce, financial services, or other online interactions.</p>
13	Meghna Jalan	Hertie School	Academia	■		■			■							<p>One critical issue in European Internet governance is the digital divide, encompassing access and literacy gaps. Infrastructure disparities, especially between urban and rural areas, hinder equitable internet access. Affordability challenges further limit lower-income individuals, perpetuating social and economic inequalities. Access alone is insufficient; digital literacy skills are crucial. A skills divide, particularly affecting marginalized groups, contributes to the overall problem. Education disparities exacerbate the issue, impacting students' ability to engage in online</p>
14	Henar López	JEF ESPAÑA	Other	■		■		■								
15	Rokas Danilevicius	Ministry of Foreign Affairs of Lithuania	Government			■			■				■			<p>"Navigating the Deepfake Landscape: Legal Regulations, Prevention Strategies, and AI Countermeasures against Information Attacks in Europe"</p> <p>Deepfakes pose a multifaceted threat to Europe, manipulating media content and risking authenticity. This disinformation method jeopardizes democratic processes, influencing elections and public opinion, undermining unity among EU states. Addressing this concern involves analyzing possible legal regulations to define deepfakes, establishing accountability frameworks, and fostering international cooperation. Prevention strategies encompass technological solutions, media literacy promotion, and platform policy analysis. Harnessing AI is crucial for content detection, attribution, and automated fact-checking. This topic would encompass a comprehensive deepfake mitigation approach, considering legal, preventive, and technological dimensions.</p>

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



- 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	Sabrina Vorbau	European Schoolnet - Insafe network	Civil society																	<p>Artificial Intelligence (AI) & Emerging Technologies.</p> <p>In cases of sextortion and grooming of minors online, AI-powered tools can make this process easier for perpetrators by allowing them to monitor social media activity on a larger scale and identify potential targets based on specific keywords, interests, or behaviours. These tools can analyse vast amounts of data and quickly identify children who may be vulnerable to manipulation. Perpetrators can use chatbots to create a false sense of trust and intimacy with children. They can initiate conversations about topics that interest the child and pretend to share the same interests. As the chatbot learns more about the child, it can use that information to tailor its responses and gain the child's trust even further. The emergence of deepfakes has introduced new risks, with deep nudes becoming increasingly prevalent. These edited versions of ordinary photos or videos that depict individuals in the nude account for 96% of all deepfakes. Sadly, more and more young people are falling prey to this technology. Deep nudes are not only used by perpetrators of financial sextortion, but also to create pornographic videos. As the technology behind deepfakes becomes more advanced and accessible, soon anyone with a phone will be able to create deceptively realistic content. In fact, AI technology is currently the only way to reliably identify deepfakes. Therefore, it is crucial that people become more aware of the potential dangers and that the topic receives greater attention.</p>
17	Sofia Rasgado Monteiro	Departamento de Desenvolvimento e Inovação Coordenadora do Centro Internet Segura, Portuguese Safer Internet Centre Coordinator – Insafe network	Government																	<p>Empowering Vulnerable Online Users. Online platforms have become essential, connecting us socially, providing information, and offering entertainment. However, they also expose vulnerable users, such as children from marginalized groups to harmful content and behavior. Reporting such incidents can be challenging due to various barriers. According to the EU Kids Online project, 42% of children have encountered harmful online content. Global Kids Online research in February 2021 concluded that offline vulnerability correlates with online vulnerability. Children at risk offline are more exposed to online risks, experience harm more frequently, and struggle to find support. Negative online content, cyber-hate, discrimination, and violent extremism are more prevalent among children with lower levels of happiness or life satisfaction, girls are more likely to be victims of online sexual solicitation, coercive sexting, and cyber-dating violence. Unfortunately, many incidents go unreported. Reporting harmful online behavior poses unique challenges for marginalized groups, children with disabilities, LGBTQ+ individuals, and immigrants, especially refugees. Discrimination and lack of support hinder their reporting efforts. Emerging tools and strategies offer promising solutions for empowering vulnerable online users to report harmful content. Some platforms have implemented "one-click" reporting features, simplifying the reporting process and others implement AI solutions.</p>
18	Lufuno T Tshikalange	Orizur Consulting Enterprise	Private sector																	<p>Access to Internet a fundamental human right</p> <p>The interconnectedness of the cyber space contributes to the persisting online vulnerabilities, requiring enhanced protection of the users' digital human rights through inter alia compulsory implementation of web security safeguards to enforcing minimum security baseline standard for digital infrastructure to capacitating users. Moreover, cross region collaboration and harmonisation of the regulatory frameworks is crucial to curb the growing pandemic of cybercrime. Considering that the GDPR has become like a de facto standard, similarly, the 2024 EuroDIG can be used as a platform to raise awareness and promote the universality of the Budapest Convention on Cybercrime.</p>
19	Wout de Natris	DC Internet Standards, Security & Safety Coalition	Civil society																	<p>Regulatory Compliance in Cyberspace</p> <p>What is the role of regulation in cyber space. Currently self-regulation is the standard. Is there a role for regulators in Europe? Does current legislation e.g. consumer protection allow regulatory oversight on digital security? Would consumers in Europe be better protected if regulators could/would step in?</p>

List of proposals for EuroDIG 2024 (as of 1 January 2024)



■ 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

23	Ilya Goessens	VUB	Academia	■								<p>I suggest the topic of desktop manufacturing as a way to empower citizens and improve digital literacy across the EU. A strongly developed desktop manufacturing 'sector' could have many benefits such as: digital/tech literacy, sustainable production; fostering innovation; and increasing European independence in production. Besides, from a guidance ethics perspective, getting involved early offers the chance to guide the moral and ethical practices in the implementation of desktop manufacturing.</p> <p>In terms of access and literacy, advancements in CAD-software and hardware (e.g., 3D-printers, CNC machines, ...), as well as open source data and designs make for a forgiving learning environment, while offering experience with different facets of digital literacy (CAD, programming, data management, electromechanics, ...).</p> <p>The flexible nature of the technology makes it possible to manufacture locally in limited quantities, as purpose-built machines are not required (capital-intensive). Rapid prototyping may stimulate innovation. Besides, we could see considerable benefits for the circular economy (right to repair movement).</p> <p>Taking into account the distributed nature of the technologies and communities underpinning desktop manufacturing, it is difficult to imagine a sound and enforceable policy that regulates what is manufactured in people's homes. Therefore, focusing on how to guide and implement the practice ethically and in line with European values rather than dwelling on the 'good' or 'bad' dichotomy may be the most constructive approach.</p>
24	Carola Croll	Stiftung Digitale Chancen / Digital Opportunities Foundation	Civil society	■			■	■				<p>Civic engagement is essential to the well-being of Europe's democracies. At the same time, the ways in which people volunteer are changing, and digital and analogue actions are increasingly intertwined. How can digital tools, especially platforms, shape and support civic engagement/volunteering? How can NPOs and other civil society institutions that rely heavily on volunteering respond to new challenges in a digital world and use it to promote their agendas and activate people? In particular, we would like to discuss the opportunities and challenges of digital civic engagement/volunteering to promote Europe-wide engagement across national borders.</p>
25	Carola Croll	Stiftung Digitale Chancen / Digital Opportunities Foundation	Civil society	■	■		■					<p>Rural areas account for around 80% of the EU's territory and around 30% of the EU's population lives in rural areas. People in rural areas face various challenges, especially in regard to digital infrastructure. We would like to discuss how to tackle the digital divide between rural and urban areas across the EU and how digital platforms can play a central role in addressing challenges, fostering local resilience and strengthening digital skills.</p>
26	Anna Romandash	Digital Democracy Centre	Academia	■		■		■				<p>Prior to 2022 Russia's invasion, Ukraine has made a significant progress in open government, Internet Governance, and effective data governance, being among the leaders in Open Data and Global Data Barometers. Yet, in 2022, the country's open government practices were halted. During the early weeks of Russia's full-scale invasion, Ukraine's government closed most of its data registries as well as changed relevant legislation to provide for more data regulations and restrictions. It also halted practices of digital declarations, procurement processes, and other important open government tools. This move strategy was met with severe criticism from the media, tech sector, and civil society.</p> <p>Under pressure, the government is reversing some of its earlier restrictions which strongly affected transparency and monitoring capacities of various watchdogs and active citizens in the country; and it's also readjusting its strategy toward Internet Governance and open government. However, Ukraine has not returned to its previous approach of transparent and collaborative data governance and digital monitoring, and the courts side with the legislators when it comes to access to certain datasets and information. State vulnerability, extreme conditions, and usage of open data by the enemy are often cited as the main reasons for such restrictions.</p> <p>This talk compares Ukraine's previous open government strategy with the one proposed by the legislators amid the Russo-Ukrainian war to show dos/donts of data managements amid crisis - and the role of citizens.</p>

List of proposals for EuroDIG 2024 (as of 1 January 2024)



- 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

27	Vita Valiūnaitė	Ministry of Foreign Affairs of the Republic of Lithuania	Government	■	■	■											<p>The Ministry of Foreign Affairs of the Republic of Lithuania would like to propose to address following digital dimension of freedom topics at the next EuroDIG meeting:</p> <ul style="list-style-type: none"> -Freedom of expression and safety of journalists, including online. -Artificial intelligence and human rights. -Fight against disinformation, hate speech and distortion of history; access to information. -Non-traditional media, progress of digital technologies, media literacy.
28	Rui Esteves	Environment General Secretary (Portugal)	Government							■	■						<p>Implementing IT Service Management (ITSM) in Public Services.</p> <p>In the present era of digital advancements, the seamless operation of government institutions relies heavily on the presence of efficient and dependable IT services. To achieve this, many public sector organizations are embracing IT Service Management (ITSM) frameworks. ITSM provides a structured approach to managing IT services, optimizing operations, and delivering high-quality services to citizens. In this article, we will explore the key steps involved in implementing ITSM in a government institution and discuss the benefits it brings.</p> <p>In Europe, Public Institutions (Government offices, General Directorates, Public Services for citizens) still have an important role in the democracy's development. We see, every day, around Europe, a lot of channels, media, services destabilizing democratic institutions with the aim of encouraging debate around topics that, in fact, add nothing to improving the quality of life of citizens. Therefore, implementing ITSM frameworks in public services will allow us to create stronger institutions that are more resistant to threats from the digital world.</p> <p>Step 1: Define Goals and Objectives Step 2: Select an Appropriate ITSM Framework Step 3: Establish an ITSM Team Step 4: Conduct a Gap Analysis Step 5: Design and Document Processes Step 6: Implement Service Desk and ITSM Tools Step 7: Training and Change Management</p>
29	Rui Esteves	Environment General Secretary (Portugal)	Government							■	■						<p>Affordable Internet Access</p> <p>Access is the ability to connect to and use the internet. This requires that people have the ability to connect physically (i.e., where they live have internet coverage) as well as the resources to use the internet. Internet access is different from availability, which refers to whether internet service is a possibility (e.g., whether or not mobile internet coverage is available where a person lives).</p> <p>Governments around the world often include language in their national broadband plans or ICT policies that call for “affordable internet access for all.” This same language is used in the Sustainable Development Goals — SDG 9c calls for universal, affordable internet access by 2020. Clearly, the importance of enabling everyone, everywhere to access and participate in the digital revolution is increasingly being recognised the world over.</p> <p>However, many of these statements are not entirely clear about what they mean by ‘access’ and ‘affordable’. This lack of clarity around what exactly we are trying to achieve can be problematic. How can we achieve a goal if we can’t measure it or if we’re all aiming for different goalposts? European companies must develop clearest guidelines and best practices fair and to be understood for all citizens.</p>
30	Rui Esteves	Environment General Secretary (Portugal)	Government							■	■						<p>DNS abuse.</p> <p>European security institutions must work actively in several settings to continually develop ways to combat and prevent DNS abuse. Draft a commitment to tackling security threats, including developing best practices, and educating the internet community. And conduct ongoing technical analysis to assess whether .com domain names are being used to perpetrate infrastructure-based DNS abuse.</p>
31	Umut Pajaro Velasquez	Youth Coalition of Internet Governance	Civil society		■		■	■									<p>Tech innovation and Governance, I think we need to discuss where is the balance between protecting Human Rights and allow experimental tech development</p>

List of proposals for EuroDIG 2024 (as of 1 January 2024)



■ 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	Javi Creus	Ideas for Change	Civil society				■	■							<p>Technological innovations don't automatically translate into social wellbeing as Daron Acemoglu states in "Power and Progress". There is a need for new social institutions which act as "compensating powers" for this to happen, for example Unions in the industrial economy.</p> <p>Data used by corporations and institutions, leveraged by AI, is the new source of power. Centralization of power on corporations offers the temptation of commercial control, when centralized in institutions opens the temptation for social control.</p> <p>UE policy fosters open software (for all) and digital sovereignty (for each one), but the combination of both misses enabling "some" citizens to act as a compensating force to power concentration.</p> <p>We need new social institutions for the collective governance of data for the common and personal good of citizens.</p> <p>We are involved in the creation of two of such new social institutions: (i) Salus.coop, citizen data cooperative for health research (ii) Datalog.es, citizen data community for planetary health.</p> <p>I believe UE should foster the development of such institutions.</p>
33	Giedre Ramanauskiene	Lithuanian Innovation Centre	Other				■							■	<p>Driven to changes in the workplace and advances in technology, remote work has become increasingly popular in recent years. But there are also new obstacles to overcome in the new reality. Businesses are now exposed to new security risks as a result of the growing popularity of remote employment. The increasing frequency of data breaches and cyberattacks has sparked worries about the security of remote work arrangements. How can the ideal environment be set up to guarantee cyber security when working remotely? Remote work offers drawbacks for employees as well. Burnout from extended work hours, feelings of loneliness, and a sense of alienation from coworkers are prevalent problems. How can the welfare of workers be guaranteed?</p>
34	Giedre Ramanauskiene	Lithuanian Innovation Centre	Other				■	■						■	<p>The digital transformation within the manufacturing sector is rapidly gaining momentum, with countries worldwide discussing not only Industry 4.0 but also anticipating the fifth and sixth industrial revolutions. Despite the high demand to monitor the digital transformation, there were no cohesive initiatives at that time to oversee industrial digitization. How can we measure digital transformation and its impact in different sectors of the economy? What should be the basic evaluation criteria? How to compare transformations in different sectors?</p>
35	Abdullah Qamar	Virtual University of Pakistan	Academia	■	■	■									<p>1. Internet for Education: I believe it would be valuable to discuss the transition from Web 3.0 to Edu 3.0. This topic explores how the Internet can be effectively utilized in the education sector.</p> <p>2. Online Safety: Ensuring the safety of children online is of paramount importance. It would be beneficial to have discussions around strategies and measures to enhance online safety for kids.</p>
36	E Cortes	IS3C	Civil society				■	■					■		<p>Recent advances in AI have led to policy discussions in regional and international fora on various governance aspects including the critical security implications and risks associated with the commercialisation and wide use of AI implementation. Taking into account ethical considerations and the dual-use, i.e. civilian and military, nature of AI, along with its potential to widen the gap between early adopting countries and non-adopters, it is necessary to stay informed and up-to-date regarding existing guidelines, principles, policies and developments related to AI on an international scale. How will the EU AI Act play a role in this global debate? Will generally accepted principles emerge when it comes to international norm development for AI? How will regional differences and preferences have an impact on these processes? How can we future-proof capacity building?</p>

List of proposals for EuroDIG 2024 (as of 1 January 2024)



■ 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

37	Carola Croll	Stiftung Digitale Chancen / Digital Opportunities Foundation	Civil society	■				■			Even though disinformation is not a new phenomenon, the widespread use of digital media can lead to a greater reach and number of circulating fake news and conspiracy theories. Disinformation, if believed by audiences, can lead to eroding trust in democratic institutions and has the potential to mobilize citizens in ways that are detrimental to modern societies. Even though many citizens generally do not believe disinformation, it can still cause damage: It creates confusion, changes the way citizens feel about certain issues and erodes trust in each other if the number of people believing in disinformation is overestimated (third-person effect). We would like to discuss the challenges of online disinformation for European democracies and upcoming elections in particular, while looking at ways to counter disinformation and improve citizens' media literacy.
38	Kim Barker	University of Lincoln	Academia			■		■			Online violence, especially online violence against women, and the digital dimension of online abuse. The phenomenon of online violence and online abuse is one which continues to rise, with increasing numbers of groups suffering extreme amounts of abusive and hateful content across online services, not just social media, but increasingly games, and virtual / augmented reality environments too. While the Digital Services Act is notionally a step forward in terms of the oversight, and enforcement provisions applicable to the spaces hosting and fostering this content, there is much more to be done, not least in light of the VAWG Directive, and the obstacles it faces. Online abuse, and online violence against women is a particular challenge in a digital society, especially one where the idea of digital safety is critical and central to participation, and equal participation. Legislative efforts have only gone so far, or only address aspects of online abuse in silos - the issue is much greater, and much wider than any one piece of law, than any one digital focussed policy, and any single online service. It is a complex, pernicious problem which affects digital citizens across regions, and requires action from internationally active stakeholders.
39	Rokas Danilevicius	Ministry of Foreign Affairs of Lithuania	Government		■	■	■				<p>Issue: "Strategic Coordination for EU Leadership in Global AI Governance"</p> <p>The issue lies in establishing the EU as a leader in shaping responsible, trustworthy, and human rights-based AI use on a global scale. This involves navigating a complex landscape of international fora, including the UN, ITU, UNESCO, OECD, and others.</p> <p>Relevance for Europe:</p> <ol style="list-style-type: none"> 1. Geopolitical Significance: AI is recognized as a geopolitical factor, impacting foreign and security policies. Europe's strategic approach ensures it plays a central role in shaping global AI governance, aligning with its values and interests. 2. Protection of Human Rights: The EU's commitment to a human-centric, risk-based, and multistakeholder approach aligns with its emphasis on protecting human rights. A global framework reflecting these principles is crucial for fostering responsible AI development worldwide. 3. Promoting European Standards: Europe seeks to lead in developing AI standards, leveraging instruments like the AI Act. This ensures the adoption of EU standards internationally, reinforcing the region's influence in shaping the rules of the AI landscape. 4. Global Collaboration: The EU aims to use its digital diplomacy as a platform to build partnerships and alliances, engaging in global discussions to guide responsible AI development. Collaboration with private sectors and global initiatives like the Global Digital Compact highlights Europe's commitment to inclusive and sustainable development of common positions and policies.

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



- 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	Farzaneh Badii	Digital Medusa	Other																		<p>The emergence of Internet-enabled Artificial Intelligence products poses challenges in Internet governance, prompting the need for inventive governance mechanisms and potential reforms to existing practices. Whether it's utilizing AI to moderate online abuse or employing the Internet for the training of AI systems, these products and systems carry implications for how the Internet is governed. We suggest exploring specific instances of Artificial Intelligence products that directly influence Internet governance for a more nuanced discussion.</p> <p>Artificial intelligence products functioning on the Internet can significantly impact online governance. An illustrative case involves the use of web crawlers in training AI products, which has noteworthy policy and technical ramifications, especially concerning web publishers and site operators globally and in Europe. Notably, several French media organizations have opted to block OpenAI's ChatGPT web crawlers. While such blanket blocking addresses concerns, it may affect content accuracy and hinder Europeans' access to knowledge online.</p>
41	Rosalind KennyBirch	Department for Science, Innovation and Technology, UK Government	Government																		<p>The WSIS+20 Review preparatory process will kick off in earnest in 2024. The multistakeholder community will need to develop an approach to the review process, considering what positive proposals we would want to see come out of the review, including a positive contribution to the SDGs; how the review process itself can be designed and implemented to encourage full participation of the multistakeholder community; consider how current multistakeholder bodies such as the IGF can be further strengthened over the next decade and beyond; and how we can pool together our networks beyond Europe to engage stakeholders from all over the world, not least from developing regions, motivating them to participate and articulate their key priorities for the review process. Implementing a WSIS+20 issues track at EuroDIG would be an excellent opportunity to bring stakeholders together to not only discuss these points, but develop a joint plan of action for approaching WSIS+20.</p> <p>The WSIS+20 Review process cuts across a number of other issues in the Internet governance space, encompassing connectivity, security and innovation, for example. However, many stakeholders engage with these issues through separate mechanisms beyond WSIS, and do not fully understand the opportunity to engage with WSIS to address these issues as well as more specific topics like the remit and function of the IGF. Upskilling the multistakeholder community on how to engage with these varied issues through a UN lens will support the process to be more inclusive and encourage the involvement of new stakeholders.</p>
42	Lina Lelesiene	STATE DATA PROTECTION INSPECTORATE OF LITHUANIA	Government																		<p>Issue: "Ethical Considerations in Artificial Intelligence and Emerging Technologies"</p> <p>Relevance: As Europe continues to embrace artificial intelligence (AI) and other emerging technologies, ethical considerations become increasingly important. This proposal aims to delve into the ethical implications of AI, machine learning, and related technologies, exploring issues such as bias in algorithms, privacy concerns, and the impact on human rights. By addressing these ethical challenges, EuroDIG can contribute to the development of responsible and human-centric approaches to the deployment of advanced technologies in Europe.</p>

List of proposals for EuroDIG 2024 (as of 1 January 2024)



- 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

43	Joel Christoph	European University Institute, Endeema, Effective Thesis	Academia															<p>The integration of intermittent renewable energy into European electricity grids is a pressing issue, directly influencing economic stability, environmental sustainability, and technological innovation. As the managing director of Endeema, I've led efforts in developing software that aligns energy consumption with renewable supply, significantly mitigating greenhouse gas emissions and energy costs. This issue is crucial for Europe to address in order to achieve a sustainable and resilient energy future, reduce dependency on non-renewable sources, and foster economic growth through innovative green technologies.</p> <p>This issue is part of the broader challenge of climate change and economic transformation. It encompasses technical aspects of grid management, economic incentives for green energy adoption, and the need for policy frameworks that support the transition to a sustainable economy. It's also related to broader social issues, such as job creation in new energy sectors and ensuring equitable access to clean energy.</p> <p>I propose a session focused on "Optimizing Energy Grids with Intermittent Renewable Sources: Economic and Technical Challenges." This will involve discussions around innovative solutions like Endeema's, policy implications, and the broader economic impact. By sharing insights from my research and start-up experience, I aim to contribute to a forward-thinking dialogue on how Europe can lead in sustainable energy integration, fostering a discussion that's both technically informed and economically grounded.</p>
44	Farzaneh Badii	Digital Medusa	Civil society															<p>Digital Trust and Safety is an evolving field that is shaping many policy and governance structures related to online content and conduct. The EU's Digital Services Act is specifically related to the field of digital trust and safety and helps shape it by setting requirements for risk assessment, transparency and other factors. The field of digital trust and safety has much to learn from Internet governance and should be mindful of human rights issues surrounding it. The issue of Trust and Safety has been discussed at EuroDIG under different umbrellas. It is timely for the community to bring its wealth of expertise under the trust and safety theme and discuss: how does digital trust and safety affect Internet governance and how can Europe and EuroDIG community align digital trust and safety practices with human rights and Internet governance values.</p>
45	Ieva Zilioniene	NRD Companies	Private sector															<p>GovTech as a Catalyst for Accelerating Public Sector Innovations</p> <p>In the era of ever-growing technology access, heightened citizen expectations for effective public services, and an expanding trove of data, governments worldwide face increasing pressure to deliver innovative solutions to complex and interconnected societal challenges. Traditional approaches to addressing these issues often prove too slow and inefficient to meet the demands of the modern world. To address this challenge, governments are increasingly exploring strategies to foster and expedite the adoption of innovative technologies within their public sectors. Lithuania has emerged as a pioneer in this endeavor, establishing the GovTech Lab in 2019. GovTech Lab Lithuania is a team in public sector focused on encouraging the creation and use of innovative solutions for the government. This dedicated team within the public sector collaborates with both public institutions and startups and SMEs to identify and address challenges through emerging technologies, accelerating the development of innovative solutions and driving digital transformation within the public sector. Since its establishment, GovTech Lab Lithuania has already won the Innovation in Politics award in 2019, was awarded in 2020 by Project Management Institute (Lithuanian Chapter) as the Best Public Sector Project, and was selected among the best TOP 3 GovTech initiatives in the world by PUBLIC. Lithuania's expertise in GovTech is now being sought after and shared with other countries eager to emulate its</p>

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



- 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	Ieva Zilioniene	NRD Companies	Private sector												<p>Bridging the Digital Divide: The Role of Public Sector Actors</p> <p>Despite widespread efforts to promote "digital inclusion" in global, regional, and national digital strategies, the digital divide remains a persistent issue. Numerous studies have demonstrated the reciprocal relationship between digital inclusion and quality of life of individuals. Yet, the World Bank's GovTech Maturity Index Report 2022 indicates that the global digital divide is widening, with regional disparities persisting.</p> <p>For accelerating "digital inclusion" within the countries, it's crucial to exchange practical approaches. Lithuania provides compelling examples of how the state can effectively foster digital inclusion. In Lithuania, public libraries have been successfully transformed into "digital hubs" for the populace, offering free internet access and essential assistance. Various initiatives are implemented by Lithuanian public institutions to enhance the digital literacy of individuals who lack it.</p> <p>Lithuanian experts are collaborating with other countries to identify their optimal strategies for achieving digital inclusion. A prime example is a project undertaken in Kenya by an NRD Companies. NRD Companies expert team, funded by the Republic of Lithuania's Development Cooperation and Humanitarian Aid Fund, is assessing the feasibility of employing a well-established Kenya's postal network to provide access to public digital services for the digitally excluded segment of society. These national and international instances could be discussed in the dedicated session.</p>
47	Ieva Zilioniene	NRD Companies	Private sector												<p>In the era of ever-growing technology access, heightened citizen expectations for effective public services, and an expanding trove of data, governments worldwide face increasing pressure to deliver innovative solutions to complex and interconnected societal challenges. To address this challenge, governments are increasingly exploring strategies to foster and expedite the adoption of innovative technologies within their public sectors.</p> <p>Lithuania has emerged as a pioneer in this endeavor, establishing the GovTech Lab in 2019. This dedicated team within the public sector collaborates with both public institutions and startups and SMEs to identify and address challenges through emerging technologies, accelerating the development of innovative solutions and driving digital transformation within the public sector. Since its establishment, GovTech Lab Lithuania has already won numerous awards and recognitions.</p> <p>Lithuania's expertise in GovTech is now being sought after and shared with other countries eager to emulate its success in modernizing their public institutions. Lithuanian experts, both from the public and private sectors, are actively engaging with other nations to assist them in developing their own tailored approaches to GovTech adoption, tailored to their unique contexts and needs.</p> <p>This session would provide an excellent opportunity to exchange best practices and insights from diverse regions around the world, gaining a deeper understanding of the specific factors that drive these initiatives forward, along with the unifying principles that underpin them.</p>

List of proposals for EuroDIG 2024 (as of 1 January 2024)



- 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

48	Sudhanshu Kumar	Jawaharlal Nehru University	Academia	Development of IG ecosystem, Innovation & economic issues, Technical & operational issues	■	■		■	<p>Developing robust ecosystem for Startups and industries</p> <p>Despite the prevalent discourse around the relatively underdeveloped European tech ecosystem and the absence of prominent "tech giants," the European Union's tech ecosystem is advancing significantly, with an unprecedented number of 'unicorns' achieving a value of 1 billion dollars. However, the European start-up ecosystem has not yet fully realized its potential due to the limited number of tech giants, particularly in the AI industry. Tech giants with extensive user bases, vast data resources, and significant financial capabilities have a clear edge in revolutionizing sectors. Google's foray into autonomous driving and Facebook's ventures into payment systems exemplify this advantage. Scaling up continues to pose challenges, including obtaining funds, the presence of diverse languages, and the fragmented nature of the Single Market. Thus, the upcoming five-year agenda should prioritize five key areas: Artificial Intelligence (AI), the implementation of a new data strategy, the establishment of pan-European innovation ecosystems, the development of a plan to regulate excessive platform power, and the adoption of a fresh approach to supporting and expanding innovation within the European Union. In this context, platforms like EuroDIG have the potential to offer sustainable and robust ecosystem services for promotion and development of new businesses and ideas.</p>
49	Mare Vahtre	Estonian Internet Foundation	Technical community			■		■	<p>Ensuring cybersecurity in the digital age has brought up the need for identification of individuals engaging with online services. The recently adopted NIS2 directive, instrumental in enhancing resilience across Europe, is contributing towards heightened cybersecurity measures. However, it presents new challenges in finding the electronic identification solutions that are effective and secure, but at the same time user-friendly and easy to manage for different organizations and companies.</p> <p>Within the last decade, several national and international identification solutions have been developed. However, some drawbacks lie in their different nature, requiring separate connections, interfaces and administrative frameworks. Besides that, widespread password-centric or authentication solutions anchored in platforms like Google or Meta fall short in collecting comprehensive user information. Moreover, they are more prone to cyber threats and attacks.</p> <p>In addition to this complexity, European entities often engage with customers all over the world, therefore, creating also the need for global solutions. The necessity is evident and we need to address the emerging challenges and facilitate widespread accessibility by finding secure and flexible solutions for electronic identification.</p>
50	Vittorio Bertola	Open-Xchange	Private sector			■		■	<p>- Implementing the Digital Markets Act, Year 2</p> <p>The new Digital Markets Act entered into force at the end of 2022; 2023 was the year devoted to identifying the gatekeepers, who now have up to March 2024 to get in line with the law's provisions. In 2023, already many issues surfaced: the designation of gatekeeper services unexpectedly excluded some (e.g. Gmail) and deferred others (e.g. iMessage). At the time of writing, nobody knows what the remedies will be: how can the other players prepare for the new competitive scenario if the plans of the gatekeepers are not known in advance? Who will ensure that the remedies are effective? We are in a learning process around techno-regulation that deserves thought and collective reflection. Can EuroDIG promote good ideas around this?</p>

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



■ 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

51	Vittorio Bertola	Open-Xchange	Private sector		■		■			■	<p>- The European Commission and SDOs</p> <p>The implementation of new European regulations on digital competition requires the adoption of new standards, for example for messaging interoperability. More generally, Europe's policies are often at odds with technological developments decided in global Internet SDOs, such as the trend to encryption. On the other hand, some SDOs have taken an active role in criticizing European regulatory proposals and lobbying the EU institutions to change them: see for example the statement by the Internet Architecture Board on the proposed CSAM regulation. How can we turn a somewhat conflictual relationship into a productive one? What is the correct subdivision of roles between the political sphere and the SDOs?</p>
52	Vittorio Bertola	Open-Xchange	Private sector				■				<p>- Open Source and product liability</p> <p>The Cyber Resilience Act and the Product Liability Directive are two new European legislative acts that for the first time impose legal liabilities and security requirements to software makers. Especially the CRA has been the subject of hot debates and frequent complaints in the open source community throughout 2023. Even if at the last minute the text was altered, still the need to comply can have a significant impact on European open source projects. Do we think that these new laws can work, or will they, as critics say, bring open software development in Europe to a halt? Is there anything that as a community we can do to make things better?</p>
53	Monojit Das	IADN	Press					■		■	<p>Issue: Countering Disinformation and Protecting Media Integrity in Europe</p> <p>Relevance for Europe: Europe faces a significant challenge in addressing the proliferation of fake news and disinformation, posing threats to democratic processes, public trust, and social cohesion. This issue is part of a larger complex involving media literacy, digital sovereignty, and safeguarding democratic institutions.</p> <p>Key Aspects and Related Issues:</p> <p>Combatting Disinformation: Challenge: Mitigating the spread of false information that undermines public trust and fuels social division. Related Issues: Developing robust mechanisms for fact-checking, improving media literacy, and fostering collaboration between governments, media organizations, and tech platforms.</p> <p>Media Integrity and Freedom: Challenge: Safeguarding the integrity of journalistic practices and protecting media freedom. Related Issues: Strengthening regulatory frameworks to counter disinformation without infringing on free speech, supporting independent journalism, and addressing the economic challenges faced by media outlets.</p> <p>Digital Sovereignty in Media: Challenge: Ensuring control over digital media platforms and content distribution while respecting fundamental rights. Related Issues: Formulating regulations that balance platform accountability, fostering domestic media innovation, and addressing cross-border challenges in regulating online content.</p>

List of proposals for EuroDIG 2024 (as of 1 January 2024)



- 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	Monojit Das	IADN	Press	■				■						<p>Freedom of media and national security</p> <p>There are lot of challenges that are arising in the media fraternity holding significant challenge to Europe at large which can be defined as follows:</p> <p>Media Literacy and Education:</p> <p>Challenge: Enhancing media literacy to empower citizens in critically evaluating information sources. Related Issues: Integrating media literacy into educational curricula, promoting public awareness campaigns, and collaborating with media organizations to educate the public on discerning reliable information. Democratic Threats:</p> <p>Challenge: Countering disinformation's impact on democratic processes and the potential manipulation of public opinion. Related Issues: Strengthening cybersecurity measures to protect electoral processes, ensuring transparency in political advertising, and fostering international cooperation to address cross-border disinformation campaigns. Relevance: Countering disinformation and protecting media integrity is crucial for Europe to maintain the resilience of its democratic institutions and uphold public trust. This issue is intricately connected to broader challenges, including media literacy, digital sovereignty, and the preservation of democratic values. By addressing threats posed by fake news and disinformation, Europe can reinforce its commitment to a well-informed citizenry, resilient democratic processes, and a media landscape that prioritizes truth and accuracy.</p>
55	Emilia Zalewska-Czajczyńska	NASK PIB	Technical community		■								■	<p>Cooperation for Cybersecurity in the European Union</p> <p>Cybersecurity is a vital issue for the European Union, as it affects the security, prosperity, and resilience of its citizens, businesses, and institutions. Thus, the EU has developed a complex legal framework to enhance its cybersecurity capabilities and resilience to cyberattacks, consisting of acts such as the NIS 2 Directive or the Cybersecurity Act. However, these regulations pose several challenges in terms of implementation, enforcement, coordination, and compliance. Moreover, the EU has to cope with the constantly evolving landscape of emerging threats and technologies in cyberspace, such as ransomware, artificial intelligence, and quantum computing. In these circumstances, cooperation between all actors and stakeholder groups involved is becoming crucial. Some good practices and instruments already exist – such as, for example, national and regional Information Sharing and Analysis Centres (ISACs) – but there is an increasing need for improvement and the establishment of new, innovative cooperation mechanisms. That is why EuroDIG could be a forum to discuss comprehensively and critically the current state and future prospects of cooperation in the field of cybersecurity in the European Union.</p>
56	Emilia Zalewska-Czajczyńska	NASK PIB	Technical community	■						■				<p>How to equip young people with the competencies necessary for the modern job market?</p> <p>Being a fresh graduate looking for the first serious job has never been easy. However, the rapid changes in the job market caused by the emergence of new technologies, such as AI, make the challenge even tougher. At the same time, technical progress is not adequately reflected in university curricula. Moreover, an increasing number of professions require the capacity to work in an interdisciplinary work environment and to combine competencies from multiple fields – for example, technical and soft skills. Meanwhile, traditional education is still often dominated by teaching knowledge in 'silos,' without equipping graduates with the ability to combine skills from different areas and collaborate with others. Given these reasons, a discourse is essential on how to prepare young people for the demands of the modern job market. How could higher education systems be adapted to better suit today's realities? Beyond these, what could be done to support graduates in acquiring the competencies of the future?</p>

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



■ 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	Emilia Zalewska-Czajczyńska	NASK PIB	Technical community				■			■	■	<p>In the search for balance between fundamental rights and security</p> <p>At a time when cyberattacks, cyberterrorism, and the sexual exploitation of children on the internet are on the rise, voices emerge about the need for increased security measures. However, some of these measures may interfere with fundamental human rights, especially the right to privacy. An instance is the heated debate in the European Union and the United States about encryption and the possibility of bypassing it in justified cases. This is why it is worth seeking answers to the questions: could fundamental rights and security be conflicting goals in certain situations? How to balance the protection of those rights with the effective prevention and prosecution of cybercrimes?</p>
58	David Frautschy	Internet Society	Technical community					■			■	<p>We need accurate data and analysis on Internet's reach, reliability, and resilience to understand how the Internet is evolving. Global Internet trends can help journalists, policymakers, civil society organisations, and everyone in-between understand the health, availability, and evolution of the Internet. Metrics on Internet technologies, Internet shutdowns, Internet resilience, and market concentration are important to have a clear picture of the health of the network. Let's gather to discuss how to obtain accurate data, how to better present it to meet the different needs of the audiences and how to go forward to ensure the right policies are put in place.</p>
59	David Frautschy	Internet Society	Technical community			■		■				<p>Threats to the Internet and what an empowered community can do about it.</p> <p>Description - The Internet is at risk. It's attributes as an open, globally connected, secure and trustworthy infrastructure for all, are being challenged by governments and corporations. Discover the new assets created by the Internet Society, helping empower the community to fight against threats to the Internet. Learn how to flag a threat, build an awareness campaign, find allies, and use the Impact Assessment Toolkit to identify the right arguments against the threats. This could take the format of a fireside chat.</p>
60	Inga Rimkevičienė	Communications Regulatory Authority (RRT)	Government		■						■	<p>EuroDIG could discuss the Side Effects of Digitalization: how we deal with them. The first aspect could be the digital inclusion of elderly people. The Internet should bring opportunities to all society groups and help to bridge divides. Lack of skills and knowledge, affordability issues, fears and threats online create new or deepen existing gaps for older internet users. Multistakeholder discussion should include the voice of communities of elderly people about challenges they face when trying to be part of digital world. The second aspect could be protection of children and young people online. Even very young children are active internet users and "smarter" than many parents or teachers. With the rapid development of digital environment, new threats emerging constantly, how/is it possible to make children safe online, what extra-efforts or new approaches are needed to achieve that. From Lithuanian perspective, we could share experience of building partnerships and engaging AI in this task. The third aspect of the discussion on the side effects of digitalization could focus on protection of internet users/consumers from any fraudulent activities that can cause financial, psychological, or any other damage. Discussion could focus on the responsibilities of different actors and readiness to walk an extra-mile in their efforts to prevent illegal/harmful activities online. Feeling protected builds trust in digital environment, and without trust digital transformation cannot progress.</p>
61	Mzia Gogilashvili	Georgian National Communications Commission (ComCom)	Government		■							<p>We propose EuroDIG discuss the importance of Media and information Literacy for Europe. This topic is offered with the vision of establishing a more sustainable and comprehensive media literacy learning environment in the EU. To raise public awareness of media literacy through a series of non-formal educational projects is crucial. Central goal of these projects should be to integrate media literacy into the formal education system, primarily in general education, recognizing the vital role that schools play in shaping responsible citizens in the digital age. But these projects should be targeted not only school and university students but also educators and parents. The primary objective of these ongoing efforts is to ensure that the new generation in the EU is well-prepared to make informed decisions in their digital lives.</p>

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



■ 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	Mzia Gogilashvili	Georgian National Communications Commission (ComCom)	Government																	<p>We are proposing EuroDIG to discuss the connectivity corridors between Europe and the Middle East and Europe and Asia that is crucial not only for Europe but for Asia, as well as South Caucasus. International internet connectivity is a critical segment of the internet service provision value chain and links each country's networks to the global internet. In an increasingly digital global economy, it enables a country's global competitiveness, analogous to international airports, seaports, or cross-border highways. Improving international internet connectivity also has positive downstream impacts on the broadband market and the wider economy through cheaper retail internet services, digital integration of services across borders (finance, trade, logistics platforms), and cybersecurity on account of redundancy.</p>
63	Rita Spínola	Security Risk Management Student Association	Civil society																	<p>The issue I suggest is The Lack of Cyber Resilience in Europe. I believe this to be still an issue in Europe, in spite of the EU Cybersecurity Strategy, since cyberattacks are frequent to infrastructure, especially since beginning of the war in Ukraine to the manufacturing industry sector. From my vantage point, this topic is of utmost importance for Europe, due to the consequences it may lead to. It is important that not only companies but also lay people become aware of potential catastrophic consequences of the simple action of clicking a seemingly-innocent link, for instance.</p>
64	Amali De Silva-Mitchell	IGF DC DDHT	Other																	<p>What is the status of greening the internet? What are examples of the use of internet and AI to help reduce waste, monitor environmental conditions, preventions and environmental crisis support? Should there be legislation that mandates greening of all internet applications where possible? What is the status of electricity and other power sources for the public? The cost of fossil fuels will go up as the resource diminishes. What is the role of the internet for the global environment what is the current status?</p>
65	Sameer Gahlot	National Internet Exchange of India (NIXI), a non-profit organisation, under the aegis of the Ministry of Electronics and Information Technology	Government																	<p>Since the time immemorial, human(s) have been constantly interacting with biotic and abiotic component(s) in our ecosystem to create this planet which is known as the Earth. In the contemporary world, they are interacting through institution(s) such as the United Nations which allow nations to interact with each other through their elected representatives. Further, to marshal the global consensus and commitment required to promote the urgently needed access of all countries to information, knowledge and communication technologies for development multi-stakeholder model(s) were designed. Though, there is a stark difference between multilateral and multi-stakeholder model(s) but both are pivotal as they act as a wheel and spoke working in tandem, capitalising on their shortcoming(s) while ensuring holistic development. One such example of multi-stakeholder model(s) include(s) the World Summit on the Information Society (WSIS), which was created is to achieve a common vision, desire and commitment to build a people-centred, inclusive and development-oriented information society where everyone can create, access, utilize and share information. The WSIS process has led to the establishment of organisation(s) such as the United Nations Internet Governance Forum (UN IGF) which facilitates discourse between ecosystem player(s) treating everyone as equals. On this note, it would be interesting to see how multi-stakeholderism would evolve in the WSIS+20 era as a high-level meeting of the UN on the overall review of the WSIS is due in 2025.</p>

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



■ 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

66	Samo Grasic	LateLab AB	Private sector									<p>The concept of Delay-Tolerant Networking (DTN) has evolved over two decades, primarily explored in academic research, labs, and space industry experiments. The surge in space missions and satellite deployments challenges the traditional "mission communication model," prompting a need for a broader discussion. DTN technology has also emerged as an Internet alternative in terrestrial applications.</p> <p>In 2023, the IETF's DTN Working Group addressed the increasing demand for DTN node identifier numbers (IPN), traditionally managed by IANA. The recent RFC (https://www.ietf.org/archive/id/draft-ietf-dtn-ipn-update-00.html) introduced Numbering Authorities for IPN management, yet specifics remain undefined, requiring multistakeholder consideration.</p> <p>Two EuroDIG discussion topics are proposed:</p> <ol style="list-style-type: none"> 1.DTN Awareness: While DTN challenges have been discussed in EuroDIG, these sessions often attract a limited audience already aware of key issues. A brief introduction during the main EuroDIG session aims to bring DTN challenges into wider focus. 2.DTN Numbering Authorities Discussion: This topic explores the formation, criteria, and rules for DTN Numbering Authorities. Crucial for accommodating diverse stakeholder perspectives, this discussion ensures a robust framework for IPN management.
67	Oksana Prykhodko	iNGO European Media Platform	Civil society									<p>Integration of national IG ecosystems into regional and global ones. How many European countries have their own national IGF? Youth IGF? How are these national IGFs and Youth IGFs involved in EuroDIG? NRIs? How many countries have EURALO ALSes? ISOC chapters? Are these structures involved in national IGFs? EuroDIG? NRIs? How do national IGFs influence national/regional/global policy developments? What are the ways forward?</p>
68	Piotr Słowiński	NASK PIB	Technical community									<p>In an era where digital transformation is accelerating, the cybersecurity is more critical than ever, especially in the face of escalating cyberthreats. It is a transnational issue that impacts i.a. the internal market, public safety, and the rights' protection. The EU NIS Directive has been a cornerstone in establishing a baseline for cybersecurity across member states, aiming to enhance the overall level of cyber resilience. Its harmonization efforts have been instrumental in mitigating cross-border cyber risks and ensuring a coordinated response to incidents. As we advance towards the NIS 2 Directive, it is crucial to build on this foundation, address the evolving cyber threat landscape, and ensure that national cybersecurity systems are both user-friendly and robust against potential attacks. The discussion should include evaluation of the NIS Directive including impact on public and private sectors or establishment of CSIRTs and European-level cooperation groups, as well as developing user-friendly and secure national cybersecurity systems including need for cybersecurity measures that are accessible and manageable for users without compromising on security. Another key issue is to discuss policy recommendations for smooth and harmonious implementation of the upcoming NIS 2 Directive including preparing of national cybersecurity strategies and recommendations for fostering a culture of cybersecurity awareness and preparedness among all stakeholders.</p>
69	Piotr Słowiński	NASK PIB	Technical community									<p>Europe's digital landscape is a complex ecosystem where security, defence, economic interests, and citizens' rights intersect. The European Union's strategies and directives highlight the importance of a resilient cybersecurity infrastructure. But the defence sector's involvement in cybersecurity is pivotal, given the rise in state-sponsored cyber activities and the need for a coordinated defence mechanism at both national and EU levels. Cyberdefence and cybersecurity, while distinct, are interconnected concepts that require a harmonized approach to ensure the security and resilience of national and European digital infrastructures. Yet the terms 'cyberdefence' and 'cybersecurity' are often used interchangeably. The discussion is needed to clarify these concepts, explore their interrelation, and examine the role and position of the defence sector within the broader national cybersecurity environment, with a particular focus on the European context. Key discussion points should include addressing defence sector's role in cybersecurity and EU's approach to cyberdefence as well as challenges including leveraging advanced technologies and intelligence-sharing for effective cyberdefence or developing clear guidelines for the harmonization of cyberdefence into national cybersecurity policies and enhancing collaboration among EU member states to address cyberthreats between defence and non-defence sectors.</p>

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



■ 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

70	Piotr Stowiński	NASK PIB	Technical community		■					■	■	<p>Artificial Intelligence (AI) is transforming the digital landscape, offering innovative solutions across various sectors. However, the integration of AI also introduces new cybersecurity challenges. AI technologies are increasingly embedded in critical infrastructure or other systems and services. As AI systems become more complex and widespread, ensuring their cybersecurity is paramount to prevent malicious exploitation that could lead to significant disruptions. The EU's approach to AI regulation, including the proposed AI Act, underscores the need for secure and trustworthy AI. There is a need for a discussion in the areas of cybersecurity risks in AI systems, including identifying potential vulnerabilities in AI and AI-based solutions or assessing the impact of cyberthreats on their integrity and reliability. Other key discussion points include introducing EU legislative and standardization frameworks for AI cybersecurity. By proactively addressing the unique challenges posed by AI technologies, the EU can ensure the resilience of its cybersecurity systems and safeguard the benefits of AI innovation. In particular there is a need for a comprehensive and coordinated approach that integrates cybersecurity considerations throughout the AI lifecycle. Especially since the cybersecurity of AI and AI-based solutions is and will be a critical aspect of Europe's digital future.</p>
71	Sudhanshu Kumar	Jawaharlal Nehru University	Academia		■					■		<p>In the area of green internet governance, the European Union faces significant obstacles. The EU's goals for sustainable internet practices are seriously hampered by the large energy consumption of data centers, the lax regulation of e-waste management, and the lack of unified rules. The situation is made more difficult by the need to strike a compromise between environmental concerns and widespread internet access. It is advised to take a holistic approach to address these issues, which includes boosting international cooperation, enforcing stricter regulations, encouraging the circular economy, and investing more in energy-efficient technologies. In order to promote a more environmentally friendly and sustainable environment in internet governance, the EU must address these challenges. The quantity of energy used by computing operations across several domains can be decreased by investing in technologies like edge computing, smart grids, and decentralized servers. Platforms like as EUROdig will establish a means by which specialists can interact with one another to address issues related to green internet governance. It will enhance the optimal approaches linked to the resolution of computation, energy, and regulation in order to create more favorable conditions for the growth of a sustainable internet.</p>
72	Sudhanshu Kumar	Jawaharlal Nehru University	Academia	■		■					■	<p>The EU AI Act may strengthen legal safeguards for those affected by AI systems. It listed a number of "high-risk uses" of AI in its original version, such as the employment of AI systems for monitoring students, determining who is eligible for welfare benefits, evaluating job seekers, and determining creditworthiness of consumers. Developers and implementers of such "high-risk" AI are required by law to guarantee the security of their systems, abstain from discriminatory bias, and make their operational manuals publicly available. Nevertheless, a risky loophole included to Article 6's high-risk classification process will negate these advantages.</p> <p>The AI Act will give AI developers the option to choose to exempt themselves from all substantive regulations for high-risk systems, assuming the modifications to Article 6 are not overturned. The AI Act would: - Create significant legal ambiguity regarding which systems are deemed "high risk"; - Cause fragmentation of the EU single market due to divergent interpretations of "high-risk" among Member States; - Make it extremely difficult for Member State authorities to enforce the law because they lack the resources necessary to adequately monitor developers' self-evaluation; - Permit dishonest developers to circumvent the fundamental requirements of the law that are intended to make their systems safer and more dependable. This would hinder developers of responsible AI.</p>

List of proposals for EuroDIG 2024 (as of 1 January 2024)



- 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	ISABEL RODRIGUEZ	YOUTH IGF SPAIN	Civil society			■														<p>The EU has taken a significant stride towards safeguarding human rights through the European Declaration on Digital Rights and Principles for the Digital Decade. However, despite these efforts, the 2023 Report on the State of the Digital Decade reveals that less than half of Europeans believe the implementation of digital rights and principles in their respective countries is satisfactory, highlighting substantial shortcomings particularly in the protection of children and young people.</p> <p>The youth, faces increased vulnerability to scams, addictions, and online aggressions, contributing to the identified deficits. While countries and companies are making efforts to solve this, a need for concrete and coordinated action is needed, not only at the national or regional level but also internationally since digital companies operate worldwide. Current laws face challenges imposed by rapid technological advancement, especially in the context of the collection and use of personal data by large corporations and governments. Not only the law, but also changes in technology, social norms and the market must be considered when addressing privacy in the digital age.</p> <p>Therefore, a participatory dialogue between legislators, technologists, businesses and civil society is proposed to create a balance between privacy and other interests, such as security and innovation. This multidisciplinary approach would be key to developing effective strategies that protect privacy without stifling innovation.</p>
74	Mark Carvell	Private Independent Consultant	Private sector			■														<p>2024 will be an important year in the evolution of multistakeholder governance of the Internet and international digital cooperation. In particular, the final stage of the negotiating process for the UN Secretary-General's Global Digital Compact (GDC) will proceed in advance of the UN Summit of the Future in September 2024. Meanwhile the UN Commission on Science and Technology for Development (CSTD) will be consulting stakeholders in advance of the 20th anniversary review of the outcomes of the World Summit on the Information Society (WSIS+20) in 2025.</p> <p>Furthermore, the contribution of ICTs and digital technologies to achieving the sustainable development goals (SDGs) of the 2030 Agenda will also continue to be a major priority for global policymakers. The EuroDIG community should continue therefore to be actively engaged in these inter-connected UN processes by providing an effective and influential channel for European stakeholder consultations, and for defining consensus-based policy positions and proposals for submission as inputs into these global processes. It is recommended therefore that the programme for EuroDIG should include evolution of multistakeholder Internet governance as a main theme in Vilnius. This should include a session on how to strengthen the IGF eco-system (including the national and regional IGFs) so that it is recognised by UN member states as best-placed to take an active role in implementing the GDC and its expected specific commitments to action. Vilnius provides a timely opportunity to develop the case for this.</p>
75	Peter Koch	DENIC eG	Technical community			■							■	■						<p>Concentration as a side effect of regulation</p> <p>EU regulation aims, among other goals, to strengthen European users and service providers, where staged approaches or exemptions for SMEs strive to strike a balance. The NIS2 directive however drastically increases the regulatory requirements for 'DNS service providers', that is providers of authoritative or recursive DNS service, of any size. Not only will the sheer volume be a challenge also for regulatory bodies, it might also lead to market concentration. What is the (anti-)pattern behind this and how can we usefully measure the development?</p>
76	Roberto Gaetano	EURALO	Civil society			■			■											<p>6G</p> <p>We all remember the discussions a few years ago about 5G. The need for governance did become obvious only later in the game, when issues like proprietary technologies, potential health issues, and more came up. Now the research and development for a new generation of communication tools and services is going on, with a lot of new ideas and potential applications. Where is Europe in this process? Are we investing enough resources to be on the leading edge of the development? Is civil society - and in particular users - sufficiently aware and involved in the process, in order to be able to have their input or bound to just complain about the effects after the fact?</p>

List of proposals for EuroDIG 2024 *(as of 1 January 2024)*



- 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

77	Roberto Gaetano	EURALO	Civil society		■	■			■	Satellite communication - There is wide agreement that satellite communication, including the development of mesh networks integrating terrestrial and non-terrestrial networks (NTN), will play an increasing role in the future. However, most of the satellite communication as of today is using proprietary standards. This reminds me of the first mobile telecommunication networks that were developed and deployed by telecom operators (at the time mostly national monopolies) and how Europe came up with the GSM that revolutionised the scenario and became the world-wide accepted standard. The questions are what is being done to develop a common standard that will allow interoperability, and in particular what role has Europe in this picture., and how can users be involved in the process of defining the governance model. As an example, we could solicit a contribution by ETSI, as the point of view of the “home of the GSM” would be particularly relevant in the debate.	
78	Roberto Gaetano	EURALO	Civil society			■	■			■	Connecting the unconnected - The tremendous progress in technology is before our eyes, more and more new ideas are proposed, new applications designed, new services developed. The question is how much of this technological progress is used to bridge the gap between well-served and under-served communities. Are we only looking at bringing faster and larger throughput to provide additional services to already well served communities or are we dedicating enough resources to develop telecommunication channels and devices to connect the unconnected? For a potential session on this topic we could also solicit virtuous examples of the latter case, presenting applications of inventive technologies that have successfully applied the principle that “Internet is for everyone”.
79	Mark Carvell	Private Independent Consultant	Private sector						■		It was generally recognised in 2022 that EuroDIG has emerged as a leading forum to promote ICT sustainability and it is imperative following COP 28 in Dubai that the programme for Vilnius should include environmental impacts as a major theme. The aim in Vilnius would be to agree how to develop and implement meaningful policies and best practices for achieving a sustainable technology environment that substantially contributes to solutions for addressing the climate emergency. Furthermore, EuroDIG proposed that green digitalisation be an additional thematic area for the UN Secretary-General's Global Digital Compact, in its response to the UN Tech Envoy's GDC consultation. The meeting in Vilnius provides therefore a timely opportunity to follow through on that proposal by developing a consensus-based input into the final phase of the GDC process that would in particular a) advocate sustainable technology-by-design principles; b) define relevant key metrics; and c) agree a series of commitments to actions by industry, governments and regulators for achieving sustainable environmental targets for current and emerging Internet and digital technologies. If EuroDIG's proposal for the GDC is accepted by the UN, the European stakeholder community would be well-placed to contribute to the implementation of the relevant commitments to action contained in the GDC, and to promoting awareness of these and monitoring their implementation.
80	Luis Manuel Arellano Cervantes	Alumni association of the Master in Digital Communication Leadership (DCLead)	Academia		■			■			Social media platforms changed the traditional public sphere in Western countries. The public sphere was the place where the public formed their opinion about public issues thanks to the information of legacy media. With social media, news media lost its place as the main provider of information to the public opinion. This led to a fragmentation of the public sphere thanks to the many voices that have taken the social functions of the legacy media. In particular, journalists are losing their traditional role as communicators between publics and politics. Thanks to social media platforms, politicians can talk directly to publics without relying in the media as intermediary. This process is called disintermediation. This shifted the power to the politicians in the digital public sphere. It could be expected that the direct communication in social media between those in power and the public would be bidirectional, but this is not the case. Studies shown fragmented conversations between political elites in democratic countries, where few are setting the agenda. I propose to discuss the impact of political disintermediation in the European digital public sphere. Other line of discussion can be the disintermediation of political speech on social media during political conflict in Europe and the geographical neighborhood (e.g., the polarization caused by the EU strategy in social media during the conflict of Israel-Hamas).

List of proposals for EuroDIG 2024 (as of 1 January 2024)



■ 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

81	André Melancia	Technical Community	Technical community	■		■		■				Inclusive Internet: Decades after the creation of WCAG, most of the internet (and major sites) are not accessible for people with access issues (disabilities such as blindness or reduced vision, motor limitations preventing proper navigation in overly designed visual sites, temporary limitations, etc.). I propose a session that would cover these issues and how to guarantee equal access rights, fairness, inclusiveness, transparency and reliability. Disabilities are not limitations.
82	André Melancia	Technical Community	Technical community			■				■	■	The new AI reality: The Internet has evolved over its lifetime and the rise of AI (in content generation, in web searches, in querying information, etc.) poses complicated new challenges. This affects all areas of discussion (Privacy, Cybersecurity, Manipulation, Technical challenges, and more). I propose two different AI sessions to discuss these topics, one for Responsible AI and Ethics, and one for Technical challenges. Respectively, they should cover (1) Legal implications, privacy, safety, transparency, manipulation, accountability, and more; and (2) technical and cybersecurity concerns, "hallucinating AI" and misleading results, LLM centralised providers, open/closed source models and consequences, and more.
83	André Melancia	Technical Community	Technical community			■			■	■		Fake news and social media: It is shown that people believe the first information they receive, but reject any subsequent correction, even if repeatedly demonstrated true and contradictory to the first one. Such manipulation and disinformation (including AI deep fakes) is well visible in events such as COVID denial, Brexit and extreme-right wing fanaticism, coup attempts in the USA and Brazil, the invasion of Ukraine, and especially in the Palestine occupation. These have shown that fake news are an effective way to manipulate public opinion, permitting violations of Human Rights to be blamed on the actual victims (in the latter case for decades). In the last 3 months, millions of people worldwide have protested in cities worldwide against these kind of manipulations, to demand respect for Human Rights and that such manipulations needs to stop. Social media (such as Facebook and Instagram) blatantly censor their posts about Human Rights violations, siding with the oppressor, according to multiple Human Rights NGOs. What can we do to guarantee that information is not censored, that it is properly verified and shown in an impartial way, in all mediums? (including decentralised media which was a founding paradigm of the Internet). The internet should guarantee Human Rights, not help destroy them.