

EuroDIG

European Dialogue on Internet Governance

Messages from Brussels [2]* 26–27 May 2026

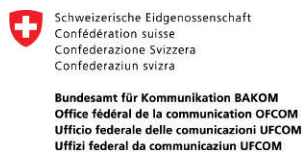
*European Voices for the
Future of the Internet*

*Celebrating 20 Years of .eu
and the Beginning of a
New Internet Governance Era*

* First “Messages from Brussels” are from 2016.



Institutional Partners



Donors



Content

Introduction

Programme

Keynotes

Opening Plenary

Messages

Main Topics

Main Topic 1 | WSIS+20 Review Outcomes and the Path to Implementation.

Main Topic 2 | European Approaches to Digital Sovereignty

Main Topic 3 | Trustworthy AI in Public Services: Transparency, Accountability, and Crisis-Resilient Communication

Main Topic 4 | Platforms' Accountability to Strengthen the Digital Public Sphere

Workshops

Workshop 1 | EUDI Wallet and EU Business Wallet as Tools for Enhancing the European Digital Single Market

Workshop 2 | Information Quality and Integrity – European Approaches

Workshop 3 | Technologies and Technical Measures to Address Online Harms

Workshop 4 | Advancing Gender Equality in the Digital Public Sphere: Tackling Online Violence and AI-Discrimination

Workshop 5 | Internet Standards and Frontier Technologies: Lessons from the Past, Tasks for Today, Choices for the Future

Workshop 6 | Youth Online Safety – Are Social Media Age Bans a Solution?

Workshop 7 | Implementing WSIS+20 Review Outcomes through Collaboration amongst European National and Regional Initiatives

Workshop 8 | Q-Day Countdown: No More Privacy?

YOUthDIG Messages

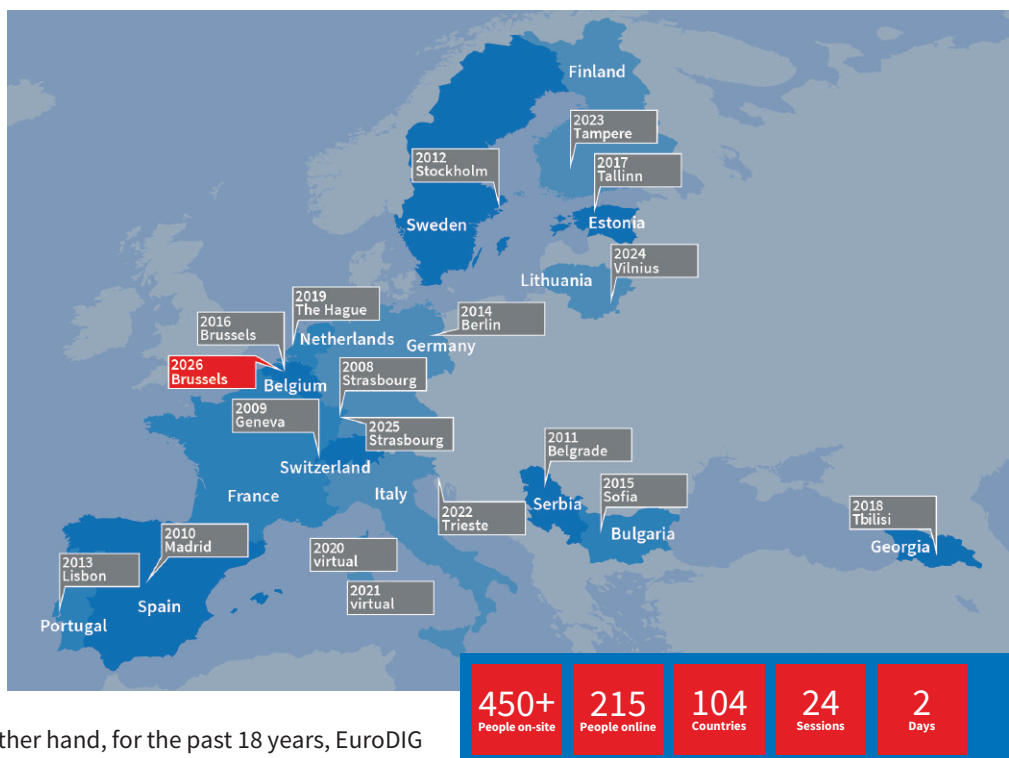
Facts and Figures

Introduction

European Voices for the Future of the Internet – Celebrating 20 Years of .eu and the Beginning of a New Internet Governance Era

The 19th edition of EuroDIG took place on 26-27 May 2026 at the Charlemagne Building of the European Commission in Brussels. It was hosted by EURid – the registry for the .eu domain name and supported by the European Commission, a longstanding Institutional Partner of EuroDIG. The event marked 20 years of .eu, celebrating two decades of the trusted digital identity. Therefore, the overarching theme for EuroDIG 2026 was “European Voices for the Future of the Internet – Celebrating 20 Years of .eu and the Beginning of a New Internet Governance Era”.

Over the past twenty years, the .eu domain and its enabling Regulation have stood as a European success story – a symbol of openness, security, and cooperation in the digital sphere. On the other hand, for the past 18 years, EuroDIG developed into a European open multi-stakeholder platform to exchange views about the Internet and how it is governed. The inclusive and continuous dialogue, which culminates in an annual event, has taken place in different European countries since its inception in 2008. For the second time we have been invited to Brussels. The programme was built in a bottom-up community approach and participants of the forum actively contributed the sessions with their expertise. The results are conveyed in the form of ‘Messages’ which are forwarded to policy makers and fed into the annual global UN Internet Governance Forum (IGF).



Programme

YOUthDIG

23 – 25 May YOUthDIG – Youth Dialogue on Internet Governance

26 May 2026

09:00 – 09:45	Pre 1 20 Years of .eu: Together Shaping Europe Online
09:00 – 10:00	Pre 4 From Deepfakes to “Nudification”: Evolving threats of Generative AI to Information Integrity and Human Rights
10:00 – 11:00	Pre 2 Europe’s Digital Backbone: Strategic Supply Chains for the Future of the Internet
10:15 – 11:15	Pre 5 Legal Professionals Navigating E-learning and AI
11:00 – 11:30	Coffee Break
11:30 – 12:30	Pre 3 Keynote – Prof. Tommaso Calarco / Quantum and Europe’s Long Term Competitiveness
12:30 – 14:00	Lunch break
14:00 – 14:30	Welcome speeches
14:30 – 15:15	Opening Plenary Democracy: Stifled or Revived by Digital Disruption of the Public Sphere?
15:15 – 15:45	Coffee
15:45 – 16:00	Introduction to EVP speech and Q&A
16:00 – 16:30	Keynote – Henna Virkkunen, Executive Vice-President European Commission
16:30 – 17:15	Intergenerational dialogue – YOU th DIG Messages
17:15 – 17:30	Wrap up
17:30 – 18:30	Cocktail reception hosted by EURid

27 May 2026

09:00 – 10:30	Main Topic 1 WSIS+20 Review Outcomes and the Path to Implementation
09:30 – 10:30	Workshop 1 EUDI Wallet and EU Business Wallet as Tools for Enhancing the European Digital Single Market
09:30 – 10:30	Workshop 2 Information Quality and Integrity – European Approaches.
10:30 – 11:00	Coffee Break
11:00 – 12:30	Main Topic 2 European Approaches to Digital Sovereignty
11:30 – 12:30	Workshop 3 Technologies and Technical Measures to Address Online Harms
11:30 – 12:30	Workshop 4 Advancing Gender Equality in the Digital Public Sphere: Tackling Online Violence and AI-Discrimination
12:30 – 14:00	Lunch break
13:00 – 13:45	Regional Consultation: Freedom Online Coalition at 15 Years: Multistakeholderism in Practice
14:00 – 15:30	Main Topic 3 Trustworthy AI in Public Services: Transparency, Accountability, and Crisis-Resilient Communication
14:30 – 15:30	Workshop 5 Internet Standards and Frontier Technologies: Lessons from the Past, Tasks for Today, Choices for the Future
14:30 – 15:30	Workshop 6 Youth Online Safety – Are Social Media Age Bans a Solution?
15:30 – 16:00	Coffee Break
16:00 – 17:30	Main Topic 4 Platforms' Accountability to Strengthen the Digital Public Sphere
16:30 – 17:30	Workshop 7 Implementing WSIS+20 Review Outcomes through Collaboration amongst European National and Regional Initiatives
16:30 – 17:30	Workshop 8 Q-Day Countdown: No More Privacy?
17:30 – 18:00	Wrap up
18:00 – 19:30	Cocktail to promote Universal Acceptance for a Multilingual Internet co-hosted by UNESCO, ICANN and EuroDIG

Keynotes

Henna Virkkunen, Executive Vice-President, European Commission

» Technological sovereignty is not about isolation. It's not about closing ourselves off. It is about Europe having the capability to develop and to maintain and to control and scale the critical technologies and infrastructures on which our economy, our security and our democracy depend. It's also preserving our ability to make strategic choices. And it's about ensuring that our values are reflected in the digital systems we rely on. And in this sense, .eu. is more than a domain name. It is a very concrete example of European digital sovereignty in practice. A trusted European digital infrastructure, a competitive European asset, and a proof that sovereignty and openness can reinforce each other.



Thibaut Kleiner, Director for Future Networks in DG Connect, European Commission

» We believe in unity through diversity. And we believe that we can invest in spaces where our strength and hopes will live for a long time. 20 years ago, .eu gave Europe a clearer identity online. Today, we have a lesson learned. It means that we can build together trusted digital infrastructure without fragmenting the Internet. We believe that sovereignty is not a threat if you design it well. It is an opportunity for all of us to share our capabilities and to become stronger. And it is an opportunity to make EuroDIG really the place where we will meet again to deserve and prepare our contributions to the next 20 years of Internet governance.



Peter Janssen, General Manager, EURid

» Open standards, interoperability, and a healthy supplier landscape strengthen resilience. ... Dependency risks grow when too much becomes tied to too few providers. In that environment, digital resilience becomes a strategic necessity. But sovereignty also exists on a personal level. In the freedom to choose and control your own digital identity. The most powerful yet simplest tool for that, is owning your own domain name. A .eu domain name gives people and organizations a European digital identity that spans borders. It works across the single market. It travels with you. It also unlocks personal digital sovereignty in a very concrete way. When you own your domain name, you own your online coordinates.



Sandra Hoferichter, Secretary General, EuroDIG Support Association

» Looking ahead, we should invest in European multistakeholder dialogue platforms that are inclusive, well-resourced and politically supported. The bottom-up approach can address the growing legitimacy gap in Europe's public policymaking. By bringing together all stakeholders on an equal footing, they create inclusive spaces for understanding complex issues, reconciling diverse perspectives and building trust through continuous, respectful engagement. While these platforms do not aim to replace parliamentary or legislative processes, they can meaningfully complement them by acting as early warning systems, barometers of societal needs and bridges between global norms and local realities.



Thomas Schneider, President, EuroDIG Support Association

» We need to make sure that the legitimate issues of concerns of our people and industries are heard and properly addressed. And we need to prove that we are able to develop solutions that offer perspective to all Europeans. Multistakeholder dialogue platforms, in particular EuroDIG, play a central role in this regard. EuroDIG allows us to identify opportunities and challenges and pave the way towards decisions that actually make things better and not worse. I'm also aware that there are voices out there that say in times where the big actors ignore rules and decide over our heads, we should also act more top-down and less inclusively. But given the democratic nature of our societies and the freedom that we want to give to our people and our industries, I do not think that this is a good idea to move away from multistakeholder cooperation. To the contrary, we need to reform and strengthen our multistakeholder structures to make them more inclusive and more effective and more politically visible at the same time.





Opening Plenary

Democracy: Stifled or Revived by Digital Disruption of the Public Sphere?

Source: <https://dig.watch/event/eurodig-2026/opening-plenary-2026-democracy-stifled-or-revived-by-digital-disruption-of-the-public-sphere>

The panel examined whether digital disruption is eroding or revitalising European democracy, framing the debate with insights from a recent youth dialogue. Claudia Luciani highlighted that governments in several member states are curtailing civil society, press freedom and using emergency powers, which together fuel democratic backsliding. She added that rapid advances in AI and disinformation campaigns threaten elections by enabling fast creation and spread of fake content, while traditional media's trust is eroding as audiences migrate to less accountable online platforms. Luciani stressed that the pace of technological change outstrips existing safeguards, calling for a responsible transformation that aligns with human rights, democracy and the rule of law.

Felix Hlatky argued that a handful of profit-driven mega-corporations dominate the internet, using advertising-based business models that extract user data and amplify polarising content. He presented Mastodon's federated network of over 15 000 servers as a concrete example of how decentralisation can restore autonomy and local moderation in the public sphere. Hlatky also noted that the speed of online lies makes timely correction difficult, underscoring the need for new moderation approaches.

Caroline Lindekamp warned that big-tech platforms exacerbate misinformation and that current efforts such as Meta's fact-checking partnership and Google's claim-review have yielded mixed results. She described the European Fact-Checking Standards Network and its work on monitoring, data-sets and media-literacy programmes as essential for building a resilient fact-checking ecosystem. Lindekamp further pointed out that many media-literacy initiatives are project-driven and underfunded, calling for sustainable financing and stronger support from European authorities.

In response to a youth question, Luciani affirmed that European institutions, through the new democratic pact and coordinated legal tools, have a central role in rebuilding trust and countering foreign interference. She and Lindekamp both stressed that existing European regulations must be vigorously enforced to be effective. The discussion concluded that safeguarding the digital public sphere will require coordinated policy standards, sustainable fact-checking infrastructure, and a shift toward decentralized, accountable online platforms.

Session Details:



eurodigwiki.org/wiki/OP_2026



youtu.be/oixm_YAxH0I



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)

Main Topic 1

WSIS+20 Review Outcomes and the Path to Implementation

Rapporteur: Mark Carvell, Internet Governance Consultant; Izaan Khan, Member of the UK Internet Governance Forum steering committee, Filip Lukáš, CENTR

1. EuroDIG supports practical actions to achieve complementarity between multi-stakeholder processes, such as the IGF and the national and regional IGFs, and UN initiatives such as the GDC, and thereby avoid duplication in the implementation of WSIS+20 outcomes. Furthermore, building on existing mechanisms within the WSIS structure for coordination, monitoring, and reporting is recommended as more resource efficient for all stakeholders, rather than investing in new processes and parallel structures.
2. Tangible steps to ensure effectiveness include: emphasising specific topics of concern to focus on (such as human rights, connectivity and the Sustainable Development Goals), cross-reporting across appropriate UN and WSIS meetings, encouraging multistakeholder policy labs and partnerships for monitoring, collaboration, and participation in multilateral fora such as the ITU Plenipotentiary, and increasing capacity-building for governmental stakeholders, in order to direct their attention to the right areas to avoid confusion.
3. EuroDIG believes that operationalising implementation of WSIS+20 should be data-driven (leveraging existing databases held by institutions, universities and other organisations) and evidence-based, supported by measurable outcomes, aligned with national and regional needs, and prioritising operational capacity. A comprehensive global roadmap, building on the existing WSIS Action Lines, and mapping actions to specific entities, would serve to ensure effective vision, coordination amongst relevant entities, clarity of purpose and accountability for actions to address priorities.
4. EuroDIG considers it important to resolve confusion about AI governance through promoting cooperation between Internet governance and AI processes, and specifically proposes the appointment of liaisons between the IGF MAG and the Independent International Scientific Panel on AI established by WSIS+20.
5. EuroDIG welcomes the UN decision to accord permanent status for the IGF; and recommends concrete actions now to be prioritised to strengthen the IGF with greater inclusivity including young people; more precision and clarity both in identifying global, regional and national priorities, and in task-setting; and more effective dissemination regionally of its concrete outputs (including those from its intersessional activities, notably the policy networks and dynamic coalitions) that inform policy decision-making processes at all levels.

Session Details:



eurodigwiki.org/wiki/MT_01_2026



youtu.be/8pmr8rBmVpQ



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://www.flickr.com/photos/195980030@N06/albums/)



Main Topic 2

European Approaches to Digital Sovereignty

Rapporteur: Paulo Glowacki, EURid Youth Committee, Izaan Khan, Member of the UK Internet Governance Forum steering committee

1. EuroDIG recognizes that Europe's dependencies on external digital technologies and infrastructures have created strategic vulnerabilities, including for democratic values. Europe must shape and self-determine its human-centric digital future while maintaining Internet openness, preserving choice of technologies and providers that adhere to open standards and interoperability, while remaining grounded in multistakeholder values and human rights.
2. Digital sovereignty is a cumulative, transformative process that requires action by all stakeholders. This effort should consist of: active industrial policy such as investment in – and the development and scaling up of – trusted European platforms and players in Chips, semiconductors, Cloud, AI, open data; supporting investment in and maintenance of open source infrastructure, interoperability, and alignment of values. This should encourage innovation, while retaining balanced regulatory approaches to key issues like procurement, competition, privacy & cybersecurity.
3. To achieve European digital sovereignty we must take a holistic approach, bringing together national policy multistakeholder efforts under a common European dimension to empower citizens, especially youth. Further, the importance of cognitive sovereignty and ensuring that European residents are afforded the ability to have a digital public sphere should be encompassed by this topic. We note the Cannes Declaration on the Sovereignty of the Mind in this regard.
4. Digital sovereignty should ultimately be interpreted to mean resilient openness and strategic autonomy leveraging Europe's strengths. Digital sovereignty should not mean isolation, stepping away from global digital cooperation, protectionism or the creation of walls that lead to fragmentation.

Session Details:



eurodigwiki.org/wiki/MT_02_2026



youtu.be/CGA9c2U4Vag



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



Main Topic 3

Trustworthy AI in Public Services: Transparency, Accountability, and Crisis-Resilient Communication

Rapporteur: Milica Vesović, Council of Europe

1. In the public sector, trust is the foundation on which effective institutions and meaningful public service are built. Trustworthy AI is therefore not only about safe technology. It is about safeguarding democratic legitimacy, human agency, inclusion, and public trust. AI should be treated as critical societal infrastructure, alongside healthcare, education, welfare, and civic communication.
2. Equality bodies and human rights institutions are essential to addressing algorithmic discrimination in public administration's use of AI, especially where information and power asymmetries affect individuals' ability to challenge harm.
3. Efficiency cannot be the only measure of success in public-sector AI. AI should improve services not only from time and cost efficiency perspective, but also make them fairer, more accessible, transparent, inclusive, and trustworthy, through human-centered design focused on citizens' rights and needs.
4. Human oversight must be real, not symbolic. Public authorities need the capacity to understand, question, override, and remain accountable for AI-supported decisions. Trustworthy AI is achieved not only through regulation, but also when fairness, accessibility, inclusion, and accountability are built in by design and experienced by all citizens in practice.
5. Human rights-based frameworks provide a foundation for trustworthy AI, ensuring alignment with democracy and the rule of law. Risk-based approaches support practical tools for risk analysis, stakeholder engagement, and mitigation of bias, exclusion, unequal access, and impacts on vulnerable groups.
6. Trustworthy AI requires strong governance, technical standards, interoperability, and digital skills. With hundreds of AI-related standards already developed globally, the challenge is to translate this expertise into practical implementation of inclusive policies. Capacity building efforts are therefore essential to help countries assess their readiness, absorb global expertise, and advance responsible, human-centred digital transformation across sectors and borders.

Session Details:



eurodigwiki.org/wiki/MT_03_2026



youtu.be/CixUYxeRI6Y



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)

Main Topic 4

Platforms' Accountability to Strengthen the Digital Public Sphere

Rapporteur: Murillo Salvador, University of Geneva

1. We consider platforms as a social digital infrastructure of democracy. Yet platforms were not designed to fulfil a civic function. Instead, they optimize engagement, e.g., through the deployment of dark patterns like infinite scrolling. They are not neutral communication and information channels: they distort the public debate by enabling the spread of disinformation. In this context, civil society acting within platform ecosystems, such as fact-checking collectives and other actors, should be supported as key partners in the digital public sphere.
2. We view the loss of cognitive sovereignty is an emerging risk linked to the embedding of AI into platforms. Algorithmic management, from recommendation systems to automated moderation, need to take into account democratic principles from the design stage and not as an afterthought. Provenance and verification mechanisms are crucial as AI-driven synthetic content and identities become more prominent in the digital public sphere, faster than regulations can be deployed. In this context, the deployment of AI tools themselves can go through preliminary steps of testing and sandboxing before reaching the market.
3. Rules do not necessarily hamper innovation. In fact, existing regulation acts as a powerful deterrent for platforms' worst outcomes in democracies. Participants called for stronger DSA compliance, and here civil society can play a key role as partners for public authorities to make platform operators accountable with regards to the law. At the same time, CoE frameworks provide foundations to expand users' agency, and international human rights provide an universal basis for users seeking to make platforms take action where no regulation exists.
4. The discussion invites us to move from consumer perspectives towards an understanding of digital citizenship as embedded in platforms. Platform design is a fluid outcome of choices. New business and engagement models should be incentivised, such as community-driven platforms that already exist and perform a civic function. At the same time, alternative forms of democratic engagement should be supported, outside of platforms, including deliberative and multistakeholder formats.

Session Details:



eurodigwiki.org/wiki/MT_04_2026



youtu.be/s_OLleJAhes



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



Workshop 1

EUDI Wallet and EU Business Wallet as Tools for Enhancing the European Digital Single Market

Rapporteur: Minda Moreira, Internet Rights and Principles Coalition (IRPC)

1. The European Digital Identity Wallet (EUDI Wallet), scheduled for implementation across all EU Member States by the end of 2026, will be a crucial and free digital identity tool that empowers EU citizens to “take back control”. It enables individuals to choose which information they share and use for online identification and authentication.
2. Similarly, the EU Business Wallet aims to address cross-border identification challenges and enable secure, seamless interactions between businesses, public authorities, and private stakeholders, enhancing trust and efficiency across the European Single Market.
3. The EUDI Wallet and EU Business Wallet must become attractive and widely adopted platforms for both citizens and businesses. Their success will depend on their ability to deliver interoperability, trust, security, and ease of use across the European Union. The key challenge is effective implementation, as these wallets can deliver significant benefits to citizens and businesses by reducing complexity, enabling cross-border interactions, and supporting regulatory compliance.
4. To ensure interoperability, trust, and security, European digital sovereignty must be embedded as an open, resilient, and collaborative approach that strengthens strategic autonomy while fostering innovation and cooperation with trusted partners.
5. To maximise impact and adoption and to avoid unnecessary duplication, the EUDI Wallet and the EU Business Wallet should be integrated into existing digital ecosystems rather than creating parallel systems. By combining interoperability, trust, and security, these wallets can become cornerstone infrastructures for Europe’s digital economy and serve as a standard for trusted digital identity solutions worldwide.

Session Details:



eurodigwiki.org/wiki/WS_01_2026



youtu.be/JZbRvqpH9V0



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



Workshop 2

Information Quality and Integrity – European Approaches

Rapporteur: Smee Cujic, Brussels School of Governance

1. AI and deepfakes pose a threat to information integrity. “Slopaganda” is increasingly being used during political campaigns to influence voters.
2. Responsibility should not lie only with users but also with media, companies, civil society organisations, NGOs and political parties. Additionally, states, government agencies, and other relevant stakeholders carry a positive obligation.
3. While labelling AI-generated content needs to serve the interest of users, it may fail to address or signal discrimination, unjust influence, social harm, or journalistic integrity. Moreover, AI content is already reshaping public beliefs and labelling it may not introduce greater clarity. It can create bias where unlabeled information is automatically perceived as high-quality or truthful, even when not wholly accurate (“implied truth effect”). At the same time, people interpret labels differently based on their background and level of critical engagement. Finally, we must raise awareness and improve human sense-making of AI-generated content, for example through media and news literacy.
4. User tools for synthetic media detection are fragmented and siloed. Currently, no universal approach exists, causing these tools to fail the moment a user moves a piece of media from one platform to another.
5. Cooperation between states requires a more unified approach. Because AI material is generated globally, vast differences across jurisdictions make it difficult to enforce control.

Session Details:



eurodigwiki.org/wiki/WS_02_2026



youtu.be/2TvuJlpE9C0



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



Workshop 3

Technologies and Technical Measures to Address Online Harms

Rapporteur: Filip Lukáš, CENTR

1. The ever-evolving nature of online harms requires a multistakeholder collaboration to be tackled effectively. This may take the form of collaboration among industry players, or cross-industry and the government.
2. Intervention on the technical layer by blocking the IP addresses or DNS have significant impact on the availability of online resources, like websites, and cause unnecessary collateral damage without necessarily addressing the illegal content in question.
3. Interventions on illegal content to increase online safety should be proportionate so that the rights of individuals are respected.

Session Details:



eurodigwiki.org/wiki/WS_03_2026



youtu.be/A2fM4gVPiFA



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)

EuroDIG
European Dialogue on Internet Governance

26–27 May
EuroDIG 2026
Brussels, Belgium

Workshop 4

Advancing Gender Equality in the Digital Public Sphere: Tackling Online Violence and AI-Discrimination

Rapporteur: Minda Moreira, Internet Rights and Principles Coalition (IRPC)

1. Advancing gender equality in the digital public sphere faces some major challenges:
 - Offline gender-based discrimination is often replicated online with changes in speed and sophistication driven by emerging technologies, driving women and girls out of the public sphere, curtailing the diversity of views, and damaging democracy.
 - Lack or limited response of the platforms and the step back from major companies on political grounds makes accountability and enforcement extremely difficult, creating an environment where perpetrators feel invincible.
 - Moderation responses often limit the right to privacy leading to deeper layers of discrimination.
2. The ideal Internet should offer a warm, friendly, engaging and accountable space that creates confidence and engagement without fear. It also fosters an environment of accountability where people speak up against online violence.
3. Multistakeholder collaboration and dialogue is essential to shape a more inclusive digital sphere built on global rules and standards, civil society led capacity-building initiatives, better education, information and preventive measures:
 - International organisations play an important role in addressing digital violence, including through standard-setting, monitoring and international co-operation.
 - Meaningful and evidence-based policy-making and regulation for online platforms need to respect the right to privacy.
 - Technical solutions need the input of those facing discrimination, particularly members of disadvantaged groups and must include safety and equality by design.

Session Details:



eurodigwiki.org/wiki/WS_04_2026



youtu.be/r-PjBnZymgY



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



Workshop 5

Internet Standards and Frontier Technologies: Lessons from the Past, Tasks for Today, Choices for the Future

Rapporteur: Filip Lukáš, CENTR

1. European stakeholders should actively contribute to global standard-setting processes aligning regulatory approaches with open, interoperable, and multi-stakeholder-driven processes.
2. Bridging the gap between standards development and real-world deployment requires coordinated action across Europe and beyond, effective advocacy with decision takers, including market and non-market incentives, e.g. through an ICT procurement process, to motivate deployment by different stakeholders.
3. To facilitate a successful adoption and deployment of standards, it is recommended to pair the standardisation process with the lifecycle of the technology and its societal implications.
4. Strengthening participation in global standards bodies calls for sustained investment in expertise, improved coordination, and support for globally diverse stakeholder engagement.
5. Human rights must be embedded in standardisation processes.

Session Details:



eurodigwiki.org/wiki/WS_05_2026



youtu.be/k0MkmiLo0F4



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



26–27 May
EuroDIG 2026
Brussels, Belgium

Workshop 6

Youth Online Safety – Are Social Media Age Bans a Solution?

Rapporteur: Desara Dushi, Vrije Universiteit Brussel

1. Blanket age bans risk oversimplifying a complex issue rather than reducing harms. It is important to fully understand the complexity of the issue which includes and requires among others child participation, hearing all expert voices, learning from international partners, and putting children's rights at the center. More viable solutions would be an age-appropriate design system, combining safety by design (with more focus on for ex. age inappropriate content and algorithms) with youth voices embedded earlier in the regulatory design and holding platforms more accountable.
2. It is important for policies to also focus on privacy, proportionality and accuracy. We need to continue the work towards harmonizing age verification measures, digital literacy and meaningful engagement with young people themselves. Any measures taken need to be centered around child rights, youth participation, and be harmonized.
3. Technical instruments to implement age bans can be privacy invasive while not guaranteeing for no more harms. There is a need to carefully assess the real-world effectiveness and proportionality of age restrictions. In terms of implementation, the technology is challenging and may negatively affect inclusion and push children towards more dangerous environments. From a security perspective regulating platforms would have a better benefits vs. harms ratio.
4. We should move away from the idea that bans will get rid of everything and change everything. Age restrictions/bans should be considered not in isolation but within current policy and regulatory context, which at European level is multi-layered and includes several national and EU level initiatives. We should be aware of the distinction between regulating access and regulating content.
5. We should be aware that this is a social issue, and the focus should not be on arbitrary age gates, but rather on mitigating the harms that users encounter through attention-exploiting, profit-driven algorithms. Digital literacy and education alone cannot help us.

Session Details:



eurodigwiki.org/wiki/WS_06_2026



youtu.be/-YczLolNnpc



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



Workshop 7

Implementing WSIS+20 Review Outcomes through Collaboration amongst European National and Regional Initiatives

Rapporteur: Mark Carvell, Internet Governance Consultant; Izaan Khan, Member of the UK Internet Governance Forum steering committee, Filip Lukáš, CENTR

1. National and regional IGFs (NRIs) are effective multistakeholder fora for implementing WSIS+20 goals, outcomes and action lines through their outreach and engagement in multistakeholder communities worldwide in support of social impacts. Collaboration amongst NRIs can include sharing best practice and national experience in agreeing priorities and messages, monitoring progress and promoting greater awareness of the importance of Internet governance in line with WSIS goals.
2. NRIs' key position in the broader Internet Governance ecosystem necessitates the implementation of innovative methods of collaboration. There should be room for experimentation in the formats of exchange and policy experimentation such as cooperative labs on topics such as emerging technologies, AI and online child protection, while preserving the bottom-up model.
3. The workshop also considered NRIs' experience in developing argument maps which provide comprehensive overviews of specific issues and policy challenges, such as age verification, covering different perspectives in support of policy decisions and geared to achieving positive impacts.
4. It was agreed that EuroDIG should maintain this dialogue on innovative mechanisms and monitor progress amongst European NRIs with periodic reviews.

Session Details:



eurodigwiki.org/wiki/WS_07_2026



youtu.be/97C1ELDvaec



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



Workshop 8

Q-Day Countdown: No More Privacy?

Rapporteur: Nicolas Zahn, Association Swiss Internet & Digital Governance

1. Loss of privacy is seen as the most pressing concern regarding digital security in the post-quantum world by the workshop participants. Q-Day is not a far-distant threat but already a partial reality, as the first successful breaks of encryption using Quantum computers show. And since post-quantum effects almost every aspect of our digital lives, we need to start today. For organizations (public and private) more clarity is needed on where encryption is currently used.
2. Technical standards are only part of the answer. We also need the awareness and resources to help organizations with the deployment of new standards. It will also need to become a part of the mindset of decision-takers, as Q-Day is a structural issue that needs coordinated actions and cannot be addressed on the individual level. In terms of responsibility for the PQC transition, participants are split between governments and service providers.
3. A potential element in a government roadmap could be capacity building for procurement officers to ensure secure-by-design ICTs.
4. Organisations must not wait and start their preparations for the PQC-transition now. Tomorrow might be too late

Session Details:



eurodigwiki.org/wiki/WS_08_2026



youtu.be/-Sr1Oman7fc



dig.watch/event/eurodig-2026



[flickr.com/photos/
195980030@N06/albums/](https://flickr.com/photos/195980030@N06/albums/)



YOUthDIG Messages



Ethics and Internet Governance

1. Ethical data governance and leak prevention
To prevent data leaks, combat unauthorized surveillance, and ensure the safety of publicly owned data, we must establish clear data ownership and strict consistency in who and what manages this information. This requires a robust multi-stakeholder approach to enforce ethical internet governance standards and protect citizens' privacy from invasive surveillance practices.
2. Inequalities and access to a safe digital environment
To prevent data profiling such as in employment or education (scholarships), we must regulate how AI algorithms are trained with our data, to avoid bias. Particular attention should be paid to the targeting through harmful and illegal practices (based on status) of vulnerable groups such as women, LGBTQ+ community and minorities.
3. Multi-stakeholders: implementations & regulations
How can companies enforce regulations, how can users implement them and how should governments monitor them? All relevant stakeholders, from governments to big tech and everyday users of digital spaces/platforms, should work together so that policies don't just stay on paper but actually work in the real world.
4. Putting people first in the age of AI
We need to make it clear that real people and their jobs should be valued more than any AI tool or technology. To keep the workplace safe and fair, governments and companies must put in place strong regulations that protect workers from being easily replaced or left behind.

Digital Impact on Children

1. Children should learn about digital literacy and be empowered with agency and critical thinking skills, from a young age, before having access to Generative AI tools. Parents should also be empowered to support their child's cognitive development.
2. Governments should invest in school mental health programs and collaborate with NGOs to provide professional support for children, to combat social media addiction, anxiety, cyberbullying, and other negative effects of social media.
3. Existing regulations (such as GDPR) should be strengthened to limit the collection of children data and the tracking of children online. Existing data of children online should be removed to prevent the targeting of ads.
4. Social media platforms should be tailored to the evolving capacities of children; certain features should be restricted, and more parental controls should be included to create safe online spaces for children under 16 (for example, prohibiting addictive design and enhancing content moderation).

The Youth Dialogue on Internet Governance (YOUthDIG) is a yearly pre-event to the European Dialogue on Internet Governance (EuroDIG) aimed to foster active youth participation. Young people (ages 18-30) from the pan-European region with a strong interest in Internet governance, digital policy and cooperation are working together to draft and advocate for the youth messages.

Every year the YOUthDIG Organising Team is compiled of former YOUthDIG participants who design the programme for the upcoming edition. This is a chance to reflect and improve the programme from last editions, build further connections with YOUthDIG alumni and the EuroDIG community and to provide an opportunity for young people throughout Europe to participate in the Internet Governance Ecosystem focusing on topics that are important to youth in the field.

Find out more at:
www.eurodig.org/youthdig

Disparities and Inclusion

1. Age disparities in accessibility to the digital services – right to offline services
Everyone should be included in online services or provided with suitable alternatives – older generations, marginalised groups based on their socioeconomic, migrant, and/or ethnic/Roma backgrounds. This would allow them equal access to online services, such as banking, e-commerce, and other digital government services. Strategies for equal access should be implemented through two routes:
 - Providing online services (with the above mentioned groups in mind) as well as intergenerational workshops, including intergenerational tech labs, with the goal of giving older generations the tools to use online services.
 - Providing offline alternatives to generally needed services including banking, commerce, healthcare, customer service,
2. Access to the internet and equal opportunities in rural areas
Everyone should have the right to access the internet regardless of social background, particularly when it comes to area of residence (accounting for appropriate age groups). In this sense it's necessary:
 - Ensuring that access to the internet becomes a human right, considering how this access has become an integral part of exercising other rights, including but not limited to freedom of expression, assembly and right to education.
 - Investing in internet infrastructure in rural areas to make sure that equal access to the internet is achieved, improving access to new opportunities (e.g. educational).
3. Gender disparities, violence perpetuated through AI and social media
 - Currently, generative AI and social media platforms are allowing gender-based violence and discrimination to be perpetrated. This affects minorities, women, people of color, LGBTQ communities and people with disabilities.
 - AI models' development should incorporate, across all stages, people from various communities and backgrounds.
4. Accessibility for people with disabilities
 - Ensuring that different internet platforms are designed to cater to the needs of people with disabilities. This means building in features that support people with visual, auditory, or cognitive impairments and taking them into account in initial dialogues on services development. Making sure these groups are included in formulation of AI models, to avoid biases and guarantee accessibility.
5. Data Centers and Sustainability
 - FLAP-D markets i.e., Frankfurt, London, Amsterdam, Paris, and Dublin are Europe's primary IT hubs, but data centres are not confined to these cities alone. They have expanded into wider regions across the continent, including the Nordics, and into rural parts of countries like Ireland and the Netherlands, well beyond their capital cities.
 - Data centres don't just appear anywhere. They are built in specific towns and regions where power is cheap, water is available and planning permission is easy to get. These places end up hosting the infrastructure that powers the global internet, yet the communities living there rarely had a say in it, and even more rarely benefit from it.



- When a hyperscale facility moves in, local electricity prices rise. Water tables shift. Grid capacity that once served homes is redirected. The people living there carry a real, material cost for infrastructure decisions made thousands of miles away, by companies they have no relationship with.
 - This is not just an environmental issue, but rather a disparity issue. Therefore, to counter it, we should design better policy that takes into account local communities and environmental impact, making sure that there's transparency behind the building processes of these centers.
6. Human Rights / protecting people
- Stronger measures must be taken to protect people in the AI labour force, including those who extract resources and those who moderate content, labour usually outsourced outside of Europe by European companies, often with little oversight or accountability.

Freedom of Expression and Disinformation

1. Increased state-led surveillance amplifies fear of self-expression. To ensure that states do not abuse their digital competencies, we put forward both immediate action and long-term solutions to combat online surveillance.

Considering the lack of international legislation regarding the ability of states to conduct surveillance, we believe that developing state-surveillance policies is critical to ensuring and maintaining citizens' safety and right to freedom of speech. We would encourage / ask international bodies such as the EU to develop regulations that could implement checks and balances on states' surveillance mechanisms. While establishing an agency responsible for such missions would be ideal, we acknowledge that the processes needed to create such an agency are extensive and require lengthy measures. This is why we advise for international legislation to be developed first, with the goal of creating and appointing an international independent body that could later take responsibility for supervising state surveillance issues.

The necessary steps for the establishment of such an independent (intergovernmental) institution should be rapidly taken. Such an agency would have the authority to regulate state-surveillance and tackle related citizens' privacy concerns.

2. More and more individuals request medical advice from Artificial Intelligence Chatbots. These proceed to giving advice on medical issues with reduced visibility on the sources that were utilised, particularly when the sources are anonymous comments from online communities.

To tackle this, we believe that AI chatbots should clearly specify the sources it used at the beginning of the response, to facilitate users' understanding of differences between professional advice and advice originating from platforms users' comments. Sources should also be written simultaneously per advice / idea expressed. While we acknowledge that there is a bibliography included in generative AI responses, we believe that health-related issues advice shall specifically mention whether the advice is coming from medical experts to avoid worsening of symptoms.

3. Social media platforms and online communities are still flooded with too much harmful / hate-speech content.

We support the idea of Implementing (AI?) algorithms that would detect harmful content (slurs, offensive words, death threats) / messages before being sent. These would notify the sender / person who is about to comment that what they are writing will be flagged as harmful, offensive etc. It would not censor the messages, allowing the users to proceed, however it would flag the comments once they are posted. After the comments are posted, they would be reported and verified against harmful content moderation and removed if found too offensive.

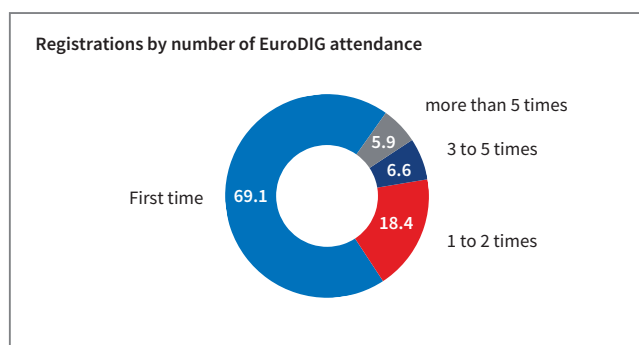
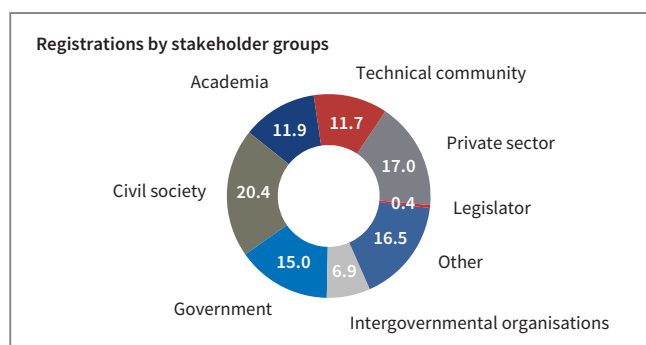
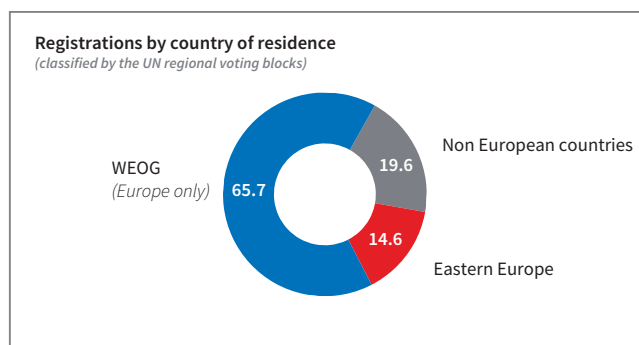
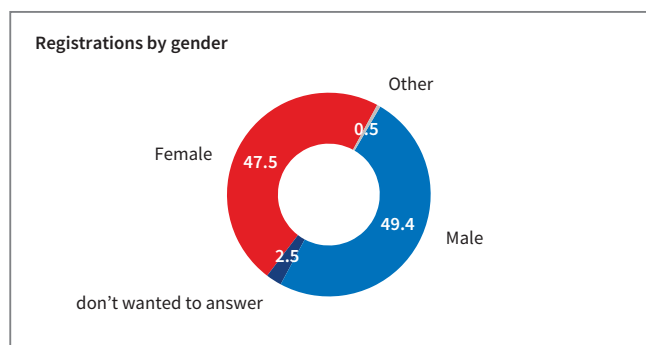
4. To combat decreased media literacy and intense spread of mis- and dis-information, we believe there should be more visibility on existing media literacy / disinformation detection campaigns and projects. There are a multitude of projects and initiatives supported by the EU which tackle the issue of media literacy and disinformation, and offer trainings and workshops. However, these do not reach the target audience. The EU could allocate financial support to increase the visibility of such projects and ensure that more people are aware of their existence. This can be done via more social-media publicity. In the long-term, we advise that such visibility campaigns could reach people who do not have access to the internet, but are still affected by disinformation. Such campaigns could involve media literacy educational materials sent via post.
5. It is increasingly difficult to distinguish AI generated images and videos from real ones. This can further increase the spread of disinformation or addictive behaviour. Therefore, we believe that labelling AI content (images and videos) on social media should be mandatory and clear to limit the spread of disinformation.



Facts and Figures

Breakdown of Registrations and Participation

We received overall 1115 registrations. The following breakdown is based on these numbers. It resulted in about 450 onsite participants (+ an undefined number of accredited employees from the European Commission) and 215 individuals joined online.



All figures in percent

The post-event analysis showed that 215 different people logged on to Webex during the three days. Breakdown per room and day are shown in the table below:

Webex Rooms		
<i>Unique participants per day</i>		
	26 May	27 May
Alcide De Gasperi	109	87
Lord Jenkins	35	62
Sicco Mansholt	-	63

Live streaming was offered by the European Commission and also embedded at the EuroDIG website. We received about 250 hits for this page. In addition we provided the recordings for each session afterwards on our YouTube channel.^[1]

^[1] <https://www.youtube.com/user/EuroDIG>

Get involved!

 www.eurodig.org

 office@eurodig.org

 www.facebook.com/eurodig

 www.youtube.com/user/EuroDIG

 www.linkedin.com/company/eurodig

 www.eurodig.org/about/newsletter

Imprint

Published by:

EuroDIG Support Association · Schächlistrasse 19 · CH-8953 Dietikon

email: office@eurodig.org · web: www.eurodig.org

Graphic and production: monade · agentur für kommunikation GmbH, Leipzig

Pictures

Title, header on pages 9 to 22: iStock.com | arsenisspyros,

page 4, 7, 8: Fred Guerdin, fred@guerdin.com