IGF Italy Committee

IGF Italy

Internet Governance Forum

2025 Report

Governing the digital

Open, responsible, sustainable

Rome: 16 – 17 October 2025

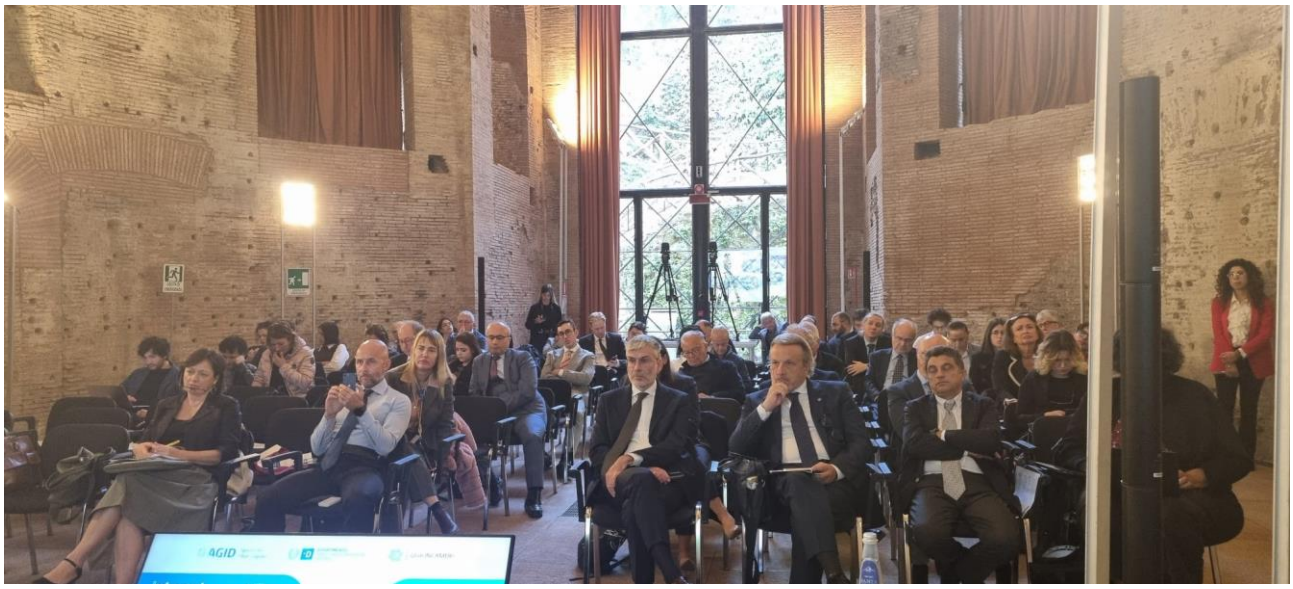
Summary

Nature and Role of IGF Italy

The Internet Governance Forum (IGF) Italy is the national multistakeholder platform dedicated to discussion and the development of proposals on Internet and digital governance policies. Recognized within the network of National, Regional and Youth Initiatives (NRIs) of the United Nations IGF, IGF Italy operates in line with the principles of openness, inclusiveness, transparency, and bottom-up participation that characterize the global model.
The Forum represents a neutral and inclusive space for dialogue among public institutions, businesses, the technical community, academia, civil society, and youth, with the aim of fostering structured and continuous engagement on evolving Internet policies and key issues of digital transformation.
Through the IGF Italy Committee, established within the Department for Digital Transformation, the Forum promotes coordination among stakeholders and supports Italy's participation in international Internet governance processes.
IGF Italy thus contributes to the development of a shared vision of the Internet as an open, global, and secure infrastructure, as well as a strategic driver for innovation and national competitiveness.

Context 2025

IGF Italy 2025 took place in Rome on 16 and 17 October 2025, hosted at the headquarters of Unioncamere and the Maker Faire, and was structured over two days of discussions under the theme "*Governing the Digital – Open, Responsible, Sustainable.*"
The first day focused in particular on governance aspects of emerging technologies, with central attention to artificial intelligence, the relationship between regulation and innovation, the role of national and European institutions, and the WSIS+20 review process.
The second day explored the integration of artificial intelligence within organizations, digital skills, and universal access to the Internet, highlighting the link between technological transformation, business competitiveness, and digital citizenship.
The connection with Maker Faire represented a distinctive feature of the 2025 edition, fostering dialogue with the innovation ecosystem and strengthening networking opportunities among institutions, businesses, the technological community, and research.
The 2025 edition therefore emerged as a structured and multi-level forum for dialogue, where regulatory dimensions, economic transformation, and skills development were examined within an integrated framework oriented toward public responsibility.



Participation

The 2025 edition of IGF Italy developed six thematic areas:

1. *Sustainability and Responsible Innovation;*
2. *Digital Skills and Inclusion;*
3. *Networks, Digital Security and Privacy;*
4. *Information, Freedom and Online Responsibility;*
5. *Digital Cooperation and Governance;*
6. *Net Neutrality.*

The programme consisted of 15 sessions held over two days, involving a total of 77 speakers/moderators (43 on 16 October and 34 on 17 October), in addition to 2 session chairs, with overall participation reaching 469 registered attendees, including 161 in person and 308 online.
In detail, 256 participants registered for 16 October (83 in person and 173 online), while 213 registrations were recorded for 17 October (78 in person and 135 online).
Across the two days, a total of 15 sessions were held (9 on 16 October and 6 on 17 October). The panels addressed a wide range of digital governance topics, including artificial intelligence, disinformation and its impact on democratic systems, cybersecurity and sustainability, digital health, skills development, international cooperation, and the WSIS+20 review process, outlining a broad and integrated overview of current challenges.
Participation included representatives from national institutions, members of the IGF Italy Committee, the Department for Digital Transformation, the Agency for Digital Italy (AgID), the Italian Data Protection Authority, academia and research institutions, as well as representatives from businesses and civil society.
Speakers also included representatives from the global IGF ecosystem—among them the MAG Chair, the IGF Secretariat Coordinator, and the NRIs Coordinator—alongside representatives from the European Commission, the Holy See, and international organizations, including remote contributions.

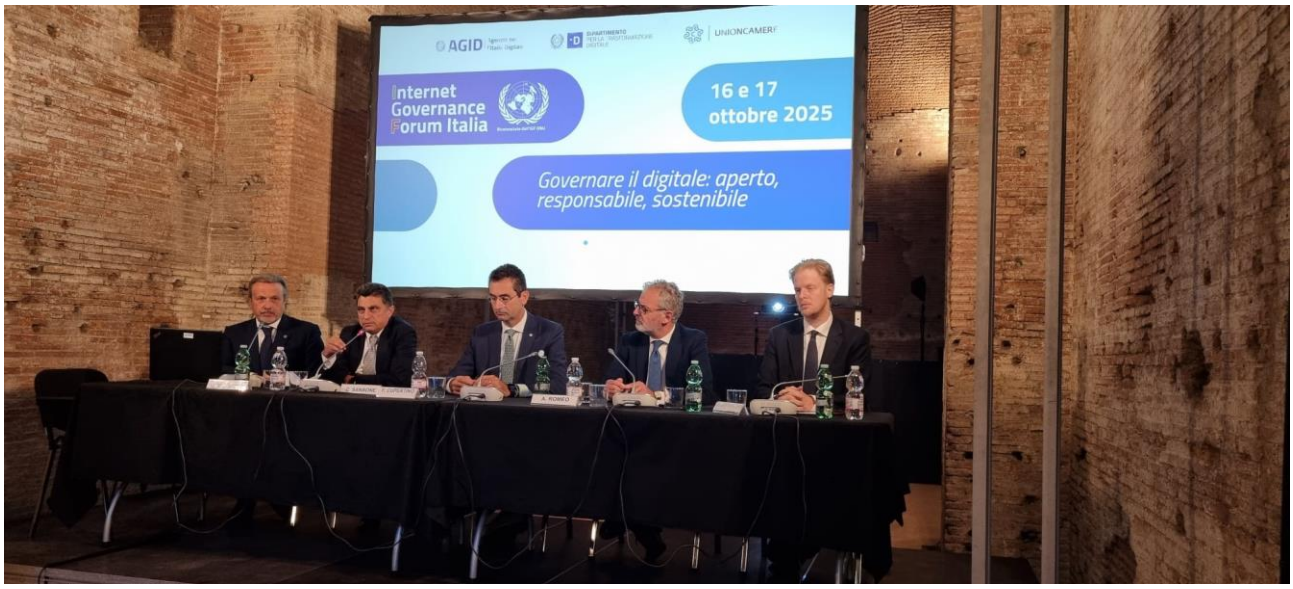
The composition of stakeholders, including youth initiatives, fostered dialogue between regulatory and operational dimensions, institutional and technical perspectives, and national and international levels, reaffirming IGF Italy's role as a structured platform for dialogue on digital governance policies.

Institutional Greetings and Opening Session

The event was moderated by **Paola Liberace** (AgID), who introduced the opening session featuring institutional remarks by:

- **Giuseppe Tripoli**, *Secretary General of Unioncamere*
- **Mario Nobile**, *Director General of AgID*
- **Monsignor Lucio Adrian Ruiz**, *Secretary of the Dicastery for Communication of the Holy See*
- **Diego Brasioli**, H*ead of the Unit for Technological Innovation and Cybersecurity at the Ministry of Foreign Affairs and International Cooperation*
- **Giuseppina Valente**, *Coordinator of the IGF Italy Committee, Department for Digital Transformation – Presidency of the Council of Ministers*

Fabrizia Benini spoke on behalf of the European Commission, addressing the role of the IGF, the WSIS+20 process, and the Global Digital Compact.
During the day, a video message from Undersecretary Alessio Butti was also broadcast, highlighting the significance of the 2025 edition in a pivotal year for the renewal of the IGF mandate.
The opening remarks framed the 2025 edition within the broader context of ongoing technological transformations and the international debate surrounding WSIS+20 and the Global Digital Compact, emphasizing the role of the IGF as a platform for cooperation and dialogue on digital policies.
The distinctive nature of the IGF as a multistakeholder platform was reiterated, grounded in an inclusive and non-binding approach capable of integrating diverse perspectives while keeping human rights and shared responsibility at its core. This model was identified as essential to avoid fragmented or purely intergovernmental approaches to digital governance.



Renewal of the IGF Mandate

The 2025 edition took place in a pivotal year for the future of the Internet Governance Forum, as the IGF mandate was under review within the WSIS+20 process, with a decision expected at the High-Level Meeting of the United Nations General Assembly held in December 2025.
It was emphasized that the renewal of the mandate represents a decisive step in consolidating the IGF as a permanent instrument for global dialogue on Internet governance, moving beyond the perception of a mere “talk shop” and strengthening its orientation toward tangible outcomes and intersessional cooperation.
The WSIS+20 review was described as an opportunity to reaffirm the value of the multistakeholder model and to ensure that the Forum continues to serve as an open, inclusive, and transparent space for dialogue on global digital policies.
During the discussions, the role of Europe in supporting a model of digital governance based on openness, protection of fundamental rights, and multilevel cooperation was highlighted.
The importance of active participation in the international debate—particularly within the WSIS+20 process—was also stressed, in order to support a model of an open Internet serving citizens and businesses, and to promote globally shared standards.
The European contribution was further linked to the need to maintain a balance between technological innovation and regulatory safeguards, ensuring that the evolution of emerging technologies, including artificial intelligence, develops in line with democratic principles and the protection of human rights.

Global IGF, WSIS+20 and the Global Digital Compact

Throughout the discussions, it was repeatedly emphasized that 2025 represents a pivotal year for the future of the Internet Governance Forum within the framework of the WSIS+20 review, which was tasked with assessing the renewal of the IGF mandate twenty years after the Tunis Agenda. This milestone was described as crucial not only for the continuity of the Forum, but also for its potential evolution in terms of strengthened institutional standing, greater influence

on global processes, and enhanced structuring of intersessional activities (NRIs, Policy Networks, Dynamic Coalitions, etc.).
The debate highlighted an emerging tension between the multistakeholder model—which has defined the IGF since its inception as an open and inclusive space for dialogue among governments, businesses, the technical community, academia, and civil society—and more explicitly multilateral approaches centered on intergovernmental dynamics. In this context, several contributions reaffirmed the need to preserve and strengthen the Forum's multistakeholder nature, considered essential to ensure plurality of perspectives, transparency, and legitimacy in digital governance decision-making processes.
The discussion also underscored the opportunity to move beyond the perception of the IGF as merely a "talk shop," by further enhancing its operational dimension and its capacity to generate substantive inputs and policy-oriented outcomes for global processes, including in connection with the Global Digital Compact and evolving forms of international digital cooperation.
Within this framework, attention was also drawn to the debate on a possible evolution in the Forum's terminology—such as the potential adoption of the name "Digital Governance Forum"—as an indication of a broader scope of action, while maintaining the foundational principles of openness, inclusiveness, and participatory engagement that define its identity.

The 2025 Debate – Thematic Lines

The debate developed during IGF Italy 2025 highlighted a structured and interconnected landscape of the main challenges in contemporary digital governance. Discussions focused on issues that simultaneously cut across regulatory, technological, economic, and social dimensions, underscoring the need for an integrated and multilevel approach.
The various sessions conveyed a complex perspective in which technological innovation, the protection of fundamental rights, security, sustainability, and international cooperation were not addressed as separate domains, but as closely interdependent elements. In particular, artificial intelligence emerged as a cross-cutting theme, both from a regulatory standpoint and in relation to its impacts on organizations, skills, and decision-making processes.
The discussions also reaffirmed the centrality of the multistakeholder model as both a working method and a guiding principle of digital governance, emphasizing the importance of maintaining open dialogue among institutions, businesses, the technical community, academia, and civil society in a phase of accelerated technological transformation.
The thematic lines that emerged over the two days are further explored in the following dedicated sections, in order to provide a systematic account of the main orientations and open issues that shaped the debate.

Artificial Intelligence and Governance

During the discussions, the centrality of artificial intelligence clearly emerged as a priority domain of digital governance, at a time when the European and national regulatory framework has recently taken on a defined and operational configuration.
The 2024 AI Act was referenced as a framework grounded in a risk-based approach, aimed at balancing the promotion of innovation with the protection of fundamental rights. Alongside this regulation, Italian Law No. 132 was described as a complementary instrument, intended to

define the national implementation system and the responsibilities of the designated authorities.

It was emphasized that the AI Act pursues a dual objective: on the one hand, fostering the development of an innovative ecosystem; on the other, ensuring that AI systems are designed and used in compliance with fundamental rights, guaranteeing safety, transparency, and ethical standards. In this context, Italy has designated AgID as the notifying authority and as a promoter of AI development within the public administration, while ACN has been assigned supervisory functions, including inspections and sanctioning powers in cases of non-compliance with security and reliability requirements.

A recurring element in the debate was the principle that safe artificial intelligence cannot exist without adequate cybersecurity measures. AI governance was therefore framed within a broader context of digital resilience and the protection of the fundamental values of both the Italian Republic and the European Union.

Human oversight was identified as an essential prerequisite. It was reiterated that "humans remain at the center" and that the human being is the ultimate reference point of the entire technological system. From this perspective, governance extends beyond the formal adoption of rules and requires the definition of control procedures, decision traceability, the establishment of audits and internal reporting mechanisms, and the ability to demonstrate responsible conduct in line with the principle of accountability.

Particular attention was devoted to critical sectors—such as healthcare, justice, employment, and electoral processes—where obligations are more stringent and where ACN is tasked with verifying compliance with high standards of security, resilience, and reliability.

The debate also highlighted the interaction between the AI Act and other European regulatory frameworks, particularly the Digital Services Act (DSA). It was noted that when AI systems are embedded within intermediary services (such as search engines, platforms, or cloud services), developers and deployers must comply with both the AI Act and the DSA, especially with regard to transparency and the management of systemic risks.

With specific reference to public administration, the need for a consistent and uniform adoption of AI was emphasized. AgID has initiated the development of guidelines for AI adoption in the public sector pursuant to Article 71 of the Digital Administration Code (CAD), with general applicability and implications also in terms of oversight, as well as additional guidelines concerning procurement and technical aspects. It was also highlighted that the effectiveness of these instruments depends on the ability to bridge the skills gap, through the introduction of specialized professional roles and appropriate training pathways.

Finally, the discussion extended to the broader issue of governing technological innovation. It was noted that every innovation requires governance, and that the balance between regulation and development must be continuously recalibrated over time. In this regard, European regulation was interpreted as a proactive approach aimed at addressing AI-related risks from the outset, while acknowledging that ongoing technological evolution will require continuous updates and adaptations.

Overall, the debate outlined a vision of AI governance as an integrated process encompassing regulatory, organizational, and cultural dimensions, requiring interinstitutional cooperation, shared responsibility, and the centrality of the human person as the guiding principle of the entire system.

AI in Businesses

The discussion on the integration of artificial intelligence into the productive system highlighted a landscape characterized by varying levels of maturity across the business sector, both in technological and cultural terms. It was noted that the adoption of digital technologies and AI remains uneven: a significant share of companies has not yet completed the transition to cloud computing, only a minority systematically uses data in decision-making processes, and a limited percentage has integrated AI into their core operations. These findings were considered in light of the European Digital Decade 2030 targets, which aim for widespread adoption of cloud, data, and AI technologies among SMEs.

It emerged that the issue goes beyond mere technological adoption and directly concerns corporate governance. Artificial intelligence was described not as a simple operational tool, but as a factor that reshapes organizational models, decision-making processes, and accountability structures. In this perspective, AI governance requires the integration of principles such as transparency, accountability, and human-centricity into internal processes, translating concepts like human oversight and responsible AI into operational practice.

The theme of return on investment (ROI) was addressed beyond a purely financial dimension. The adoption of AI was linked to broader needs for competitiveness, innovation, and sustainability over the medium to long term, also in light of demographic trends and global investment dynamics, which show a concentration of technological capabilities in other geopolitical contexts.

From this standpoint, AI was seen as a strategic lever for maintaining adequate levels of productivity and competitiveness, particularly in a European context characterized by demographic constraints and limited resources.

Particular emphasis was placed on training as a strategic enabler. It was stressed that the main critical factor is not only access to technology, but the level of digital skills and the ability to use tools in an informed and responsible manner. Training was framed not only in technical terms, but also in cultural and ethical dimensions, as a prerequisite for sustainable and responsible AI use—both within companies and in their interactions with customers, employees, and citizens.

Closely related is the issue of risks associated with uninformed use. The discussion highlighted the danger of deploying AI tools without fully understanding their nature, limitations, and implications, potentially leading to uncritical dependence or flawed decision-making.

Awareness was identified as a key condition to avoid misinterpretations of technologies—for example, conflating generative AI, chatbots, and more complex systems without distinguishing their functionalities and limitations—and to prevent distortions in organizational and decision-making processes.

Finally, the debate addressed the role of SMEs and simplified tools, noting that the availability of low-cost or easy-to-implement solutions can expand access to innovation, but also requires adequate governance and skill frameworks. Without such safeguards, there is a risk of superficial adoption, disconnected from business processes and not aligned with the principles of security, transparency, and accountability outlined in the European regulatory framework.

Overall, the discussion underscored that artificial intelligence in business cannot be reduced to a discrete technological choice, but must be embedded within a broader strategy of organizational transformation, skills development, and responsible governance of innovation.

Skills, AI Literacy and Human Capital

The issue of skills emerged as one of the central pillars of the entire debate, cutting across reflections on AI governance, its adoption in public administration, and its integration into production processes. Several contributions emphasized that digital transformation cannot be addressed solely in infrastructural or regulatory terms, but requires a structural investment in human capital and digital culture. Digitalization was described as a cultural process that affects people before technologies, generating not only infrastructural gaps but also cognitive and educational divides.

Within this framework, AI literacy was identified as a strategic dimension of digital citizenship. It was stressed that educating individuals about artificial intelligence means enabling them to understand how it works, its limitations, and its ethical and social implications. Awareness emerged as the key concept: to effectively use a tool, one must first understand it—recognizing that generative models and large language models do not "know" or "understand," but produce outputs based on probabilistic mechanisms.

AI literacy was articulated along two complementary dimensions: a technical-practical one, aimed at preventing misinterpretation and misuse, and an ethical one, addressing issues such as transparency, bias, sustainability, privacy, and the impact on democracy.

At the same time, the debate highlighted the risks of uncritical use of digital tools, which may affect cognitive capacities and individual responsibility. The need to build a shared sense of social responsibility—particularly with regard to younger generations—was emphasized, ensuring that the use of AI supports rather than replaces critical thinking.

From this perspective, AI education was not framed as a purely technical competence, but as a broader process of cultural development and ethical awareness.

With specific reference to public administration, it was noted that awareness must go hand in hand with competence. The need for a conscious use of AI—grounded in an understanding of both risks and benefits and supported by technical regulation and institutional coordination—was strongly emphasized. However, it was also acknowledged that specialized skills remain insufficient and that structured AI-related roles are still lacking within administrative bodies.

The introduction of new professional profiles in recruitment plans was identified as a first step toward achieving a level of specialization aligned with the demands of technological innovation.

The debate also linked the issue of skills to the competitiveness of the productive system. It was observed that a significant portion of the population still possesses limited basic digital skills, a gap that is also reflected in the SME sector. In a context where European 2030 targets call for widespread use of data, cloud, and AI, training was identified as an essential lever for supporting innovation and economic resilience.

Looking ahead, AI-related skills are expected to significantly impact organizational models and work processes. The adoption of AI was described as a transformative factor requiring a rethinking of decision-making flows, roles, and responsibilities, translating into practice principles such as human oversight and accountability.

This implies not merely the introduction of technological tools into existing procedures, but a broader redesign of processes in line with new capabilities and regulatory and ethical constraints.

Overall, the discussion portrayed a transformation that simultaneously affects education, work, and organizations. AI-related skills were not presented as ancillary abilities, but as a structural condition for ensuring a conscious, secure, and responsible use of emerging

technologies, consistent with the principles of human centrality, protection of rights, and sustainable innovation that guided the entire 2025 edition.

Data, Interoperability and Security

Throughout the discussions, it was repeatedly emphasized that the governance of artificial intelligence—and, more broadly, digital transformation—cannot be separated from robust data governance, adequate levels of interoperability, and a structured approach to cybersecurity. Data were described as an enabling infrastructure for decision-making processes and AI applications, highlighting the importance of open data policies and the harmonization of obligations across public administrations. The evolution of the national open data portal and the significant increase in the number of administrations publishing datasets were identified as signs of progress, albeit within a still uneven landscape marked by territorial and organizational disparities.

The issue of interoperability was addressed in connection with the broader European regulatory framework and the need to ensure coherence across different regulatory domains, such as the interaction between the AI Act and the Digital Services Act. In this context, it was emphasized that the flexibility of the regulatory framework is intended to encompass rapidly evolving technological applications, ensuring transparency and the management of systemic risks, even when AI is embedded within intermediary services. Interoperability was therefore understood not merely as a technical issue, but as a legal and organizational condition for a coherent and integrated digital ecosystem.

Cloud computing was identified as a key component of infrastructural modernization, both in public administration and in the productive system. However, it was noted that cloud adoption remains partial, with only a portion of companies having completed this transition. The infrastructural dimension was also linked to geopolitical dynamics and international investments in AI, particularly the concentration of technological capabilities in other global contexts. In this perspective, the issue of technological sovereignty was implicitly connected to the need to strengthen Europe’s capacity to innovate, invest, and govern its own digital infrastructures.

Cybersecurity was identified as a fundamental prerequisite of the entire system. It was explicitly stated that secure artificial intelligence cannot exist without adequate cybersecurity measures. The National Cybersecurity Agency (ACN) was identified as the competent authority for oversight, with inspection tasks and sanctioning powers in cases of non-compliance with security and reliability requirements. In critical sectors—such as healthcare, justice, employment, and electoral processes—these obligations are further strengthened, requiring high standards of resilience against cyber threats.

Overall, the debate outlined an integrated vision in which data, interoperability, and security are closely interconnected dimensions. The quality and sharing of data fuel artificial intelligence; interoperability ensures coherence and continuity across systems and regulatory frameworks; cybersecurity guarantees reliability and the protection of rights. Only a balanced integration of these components can support a digital development that is open, responsible, and aligned with the fundamental values emphasized throughout the 2025 edition.

Democracy, Information and Social Cohesion

The discussions strongly highlighted the democratic dimension of digital transformation, particularly with regard to the role of public institutions, the quality of information, and the resilience of social cohesion. It was emphasized that digitalization is not merely a technical process, but a phenomenon that affects individuals, social relationships, and the balance between public and private actors. In this context, the need for public administration to maintain an active and qualified role in digital governance was implicitly reaffirmed, avoiding risks of marginalization or loss of centrality in relation to global technology actors.
A central theme concerned the risk of disinformation and information manipulation through the use of artificial intelligence. It was noted that the AI Act explicitly addresses the production or manipulation of content capable of distorting the information environment, thereby impacting civic debate and democratic processes. In this perspective, AI governance was linked not only to the protection of individual rights, but also to safeguarding the quality of information and the integrity of public discourse. The interaction between the AI Act and the Digital Services Act was presented as a mechanism to strengthen transparency obligations and the management of systemic risks in digital intermediary services.
The principle of human centrality was also emphasized as a guiding criterion for the entire digital ecosystem. Several contributions reaffirmed that human beings must remain at the center of technological development, promoting a governance model based on shared values, fundamental rights, and collective responsibility. This approach was presented as a distinctive feature of the European model, aimed at balancing innovation with the protection of rights.
The debate also addressed the balance between public and private actors in the development and governance of digital technologies. Reflections on the evolution of regulatory frameworks in response to previous technological innovations highlighted the delicate relationship between regulation and development. European AI regulation was interpreted as an attempt to proactively address risks, while acknowledging that innovation requires continuous adaptation and ongoing dialogue among institutions, businesses, and civil society.
Finally, the issue of social cohesion was examined in relation to digital and cultural divides affecting the country. Digital transformation was described as a process that can widen disparities among territories and social groups if not accompanied by adequate inclusion and training policies. In this regard, the multistakeholder model was highlighted as a key instrument for dialogue and collaboration among institutions, businesses, the technical community, academia, youth, and civil society, supporting the development of shared solutions and strengthening the democratic legitimacy of decisions in digital governance.
Overall, the debate demonstrated that democracy, information, and social cohesion are deeply interconnected dimensions of AI governance. The quality of public institutions, the transparency of information processes, and the capacity for cooperation among diverse actors were identified as essential conditions for ensuring technological development that is consistent with constitutional values and with the vision of the Internet as an open, responsible, and inclusive space.

Digital Health

During the discussions, digital health was addressed as a strategic domain of technological transformation, where the protection of rights, innovation, and the organization of public services are closely interconnected. A strong emphasis emerged on the need to balance the protection of health data—classified as highly sensitive—with the enhancement of their

potential for care, research, and planning purposes. The digital dimension of the individual was framed as an extension of the protection of the physical body, highlighting the importance of principles such as data accuracy, integrity, and fairness, as well as the accountability of all actors involved in the healthcare ecosystem.
Particular attention was given to the new European Regulation on the European Health Data Space (EHDS), described as a structural step toward a federated model of data sharing. The distinction between primary use of data (for care and assistance) and secondary use (for research, innovation, and health planning) was interpreted as a key organizing principle of a system aimed at reconciling interoperability with privacy protection. The approach that recognizes public interest as a legal basis for data use—combined with safeguards for citizens—was seen as an innovation likely to significantly impact national systems, requiring stronger cooperation among institutional levels and supervisory authorities.
The issue of interoperability was further developed through references to federated models of clinical data networks, in which data remain locally stored while algorithms or aggregated results are shared. This approach was identified as capable of balancing large-scale research potential, data confidentiality, and European cooperation, anticipating the principles of the emerging regulatory framework.
The integration of artificial intelligence into biomedical research was described as a high-impact transformative domain, capable of reducing time and costs in experimentation and expanding access to advanced therapies. At the same time, concerns were raised about excessive reliance on generative systems operating on probabilistic bases, with potential biases deriving from training data. This led to a clear indication of the need for transparent models, scientifically validated and subject to human oversight, avoiding uncritical automation in clinical and decision-making processes.
Finally, digital health was linked to public investment and reform policies, particularly with regard to the strengthening of electronic health records, telemedicine, and digital infrastructures. While the pandemic accelerated the adoption of remote care tools, implementation challenges remain due to regulatory delays and territorial disparities. In this perspective, digital health was identified as a lever for more effective planning, prevention, and the strengthening of equity across territories, with the goal of ensuring a system that is inclusive, interoperable, and sustainable.

Net Neutrality

During the discussions, the issue of net neutrality was addressed within the broader reflection on Internet governance as an essential infrastructure for the exercise of rights, economic development, and democratic participation. Net neutrality was framed as the principle that data traffic must be treated fairly and without discrimination, preventing practices that may favor or disadvantage specific content, services, or operators, thereby distorting competition and access to information. This approach aligns with the European model, which emphasizes the protection of fundamental rights, human centrality, and the promotion of fair competition.
The discussion highlighted that net neutrality is not merely a technical issue, but a structural component of the democratic quality of the digital space. An open and neutral ecosystem based on equal treatment is essential for ensuring informational pluralism, enabling barrier-free access to the digital market, and protecting users from concentrations of economic or technological power. In this sense, net neutrality was implicitly linked to the need to maintain

a balance between innovation and regulation, avoiding both deregulatory approaches and excessive rigidity, in line with the idea that technological innovation requires adaptive governance tools over time.
The topic was also connected to the interaction among different European regulatory frameworks that impact transparency and the management of systemic risks in digital services. In this context, net neutrality extends beyond the regulation of access infrastructures, encompassing the overall functioning of the digital ecosystem and the responsibilities of the actors involved.
The reference to the multistakeholder model reinforced the idea that net neutrality must remain the subject of continuous dialogue among institutions, businesses, the technical community, academia, and civil society. Its protection was implicitly framed as a shared responsibility, essential to ensuring the development of the Internet in line with principles of openness, inclusion, and sustainability. In this perspective, net neutrality remains a cornerstone of Internet architecture and a fundamental reference point in multilevel digital governance policies.

Youth Participation

Youth participation represented a defining component of the 2025 edition of IGF Italy, confirming the role of Youth IGF Italy as an initiative structurally integrated into the national Internet governance process and part of the network of Youth Initiatives recognized within the United Nations IGF framework. In this context, the presence of young participants enriched the multistakeholder dialogue with a generational perspective on digital transformation and AI governance.
Within the programme, a dedicated session was held on the theme “Ethical and Safe LLMs in Education: From the Right to Education to the Protection of Human Rights,” addressing the relationship between artificial intelligence and education, with particular focus on the development of critical skills and the responsible use of generative AI tools. The session fostered intergenerational dialogue among young participants, researchers, and experts, highlighting the importance of AI literacy as a core dimension of digital citizenship.
The discussion emphasized the need to promote a deeper understanding of how large language models function and their limitations, alongside greater awareness of the ethical and social implications of artificial intelligence. It was also stressed that the use of such tools in educational pathways must be accompanied by the development of critical thinking and individual responsibility, ensuring that AI supports learning processes without replacing personal cognitive effort.
The active participation of young people reaffirmed the relevance of IGF Italy as an open and inclusive platform for dialogue, where new generations can meaningfully contribute to shaping digital governance policies and to developing a shared vision for the future of the Internet.
Conclusions
The conclusions of the 2025 edition were framed within a context marked by profound regulatory, technological, and geopolitical transformations, highlighting the need to consolidate the role of IGF Italy as a national platform for structured dialogue on digital governance. Several contributions emphasized that the current moment requires a conscious approach to governing innovation, avoiding both deregulatory tendencies and excessive rigidity

that could hinder development, in the awareness that every innovation requires governance tools capable of adapting over time.

One of the key priorities for 2026 concerns strengthening Italy's contribution to the international debate, also in light of the outcomes of the WSIS+20 review, identified as a crucial milestone for reflecting on the future of the Internet Governance Forum and the multistakeholder model.

It was reaffirmed that the multistakeholder format is not merely an organizational method, but a fundamental choice in terms of democratic legitimacy and inclusiveness, capable of engaging institutions, businesses, the technical community, academia, youth, and civil society.

In this perspective, the establishment of the IGF Italy Committee by the Italian Government—an initiative unique in Europe—represents a concrete and effective response to the need for continuity and coordination among different actors, particularly at a time when issues such as artificial intelligence, data governance, cybersecurity, and digital industrial policies are becoming increasingly strategic. AI governance, in particular, was described as a process requiring interinstitutional cooperation, oversight, and coordination among competent authorities, elements that can find a stable point of convergence within the Committee at the national level.

Within this framework, the need to promote greater awareness of the IGF Italy Committee and its operational mechanisms was also emphasized, in order to encourage broader and more informed participation by all relevant stakeholders. Similarly, the importance of enhancing the visibility of the IGF Italy platform was highlighted, as it represents a key tool for information and participation, yet remains known to a relatively limited audience.

The discussions also pointed to the need for ongoing in-depth analysis of specific thematic areas, consistent with the complexity of the issues addressed. The value of technical and specialized exchanges was repeatedly underlined, particularly in light of the interaction between different European regulatory frameworks, such as the AI Act and the Digital Services Act. The establishment of thematic working groups therefore appears consistent with the approach that emerged from the debate, oriented toward a detailed and multidisciplinary analysis of technological, legal, and organizational implications.

Another strategic axis concerns widespread training. It was emphasized that digital transformation is not only a technological issue but also a cultural one, affecting individuals and organizations alike. Strengthening awareness and skills was identified as a priority both for public administration and the productive system. Training was therefore framed as a structural lever to prevent uncritical uses of artificial intelligence and to ensure that principles such as transparency, accountability, and human centrality are effectively implemented.

Finally, the conclusions highlighted the importance of Europe's positioning within a global context characterized by strong investments and international competition in artificial intelligence. European regulation was interpreted as an effort to address risks without renouncing innovation, while requiring continuous adaptation and active participation in multilevel governance processes. In this context, the national contribution can be strengthened through improved internal coordination and more qualified participation in European and international processes.

Overall, the conclusions outlined a path focused on continuity, cooperation, and institutional strengthening, confirming IGF Italy as a permanent space for dialogue and as a platform connecting **Recommendations**

Recommendations

For the Italian Government

In light of the themes that emerged during the two days of discussions, the recommendations addressed to the Italian Government align with the priorities identified in the areas of AI governance, data governance, digital security, and skills development.

Ensure coherent and coordinated implementation of the AI Act and Law No. 132.
There is a clear need to guarantee effective application of the national regulatory framework in complementarity with the European regulation, strengthening the role of competent authorities (AgID and ACN) and enhancing interinstitutional coordination mechanisms, particularly in critical sectors such as healthcare, justice, employment, and electoral processes.

Strengthen security as a prerequisite for AI development.
It was reiterated that secure artificial intelligence cannot exist without robust cybersecurity measures. It is therefore recommended to consolidate standards of security, resilience, and reliability, while supporting inspection and oversight activities under the current regulatory framework.

Promote consistent AI adoption in public administration.
Given the varying levels of maturity across administrations, it is advisable to support the uniform adoption of guidelines and technical tools developed under the Digital Administration Code (CAD), fostering a conscious use of AI based on a clear understanding of risks and benefits.

Invest in structural and specialized skills.
Strengthening skills was identified as a key condition for digital transformation. It is recommended to continue integrating specialized professional roles into public sector staffing plans and to support AI literacy and continuous training programmes, including ethical and civic dimensions.

Support the productive system in AI adoption.
Considering the uneven maturity of enterprises and the lag in the adoption of cloud, data, and AI technologies, it is recommended to strengthen support tools, training initiatives, and assistance programmes for SMEs, in line with European 2030 targets.

Enhance data governance and interoperability.
It is recommended to continue consolidating open data policies and harmonizing obligations across public administrations, ensuring coherence among the various European regulatory frameworks affecting digital services.

Safeguard the quality of information and democratic debate.
In light of the risks of manipulation and disinformation through AI systems, it is recommended to strengthen transparency tools and systemic risk management mechanisms, in coordination with the European regulatory framework.

Consolidate Italy's European positioning.
In a global context characterized by strong geopolitical dynamics and concentration of AI investments, it is recommended to strengthen Italy's participation in multilevel digital governance processes, actively contributing to the evolution of the European model based on rights, security, and human centrality.
Overall, these recommendations outline a path that integrates regulation, security, skills, and institutional cooperation, consistent with the approach emerging from the debate and with the vision of an open, responsible, and sustainable digital development.

For the IGF (United Nations)

In light of the reflections developed during the 2025 edition, the recommendations addressed to the global Internet Governance Forum are framed within the WSIS+20 review process and the broader debate on strengthening the IGF mandate, as a crucial step toward consolidating an effective multilevel governance model for the Internet and the digital domain.

Strengthen the IGF mandate in terms of continuity and institutional stability.
The debate highlighted the need to consolidate the IGF's role as a permanent platform for dialogue, moving beyond the perception of a purely consultative forum and enhancing its capacity to generate substantive contributions to global processes.

Preserve and reinforce the multistakeholder model.
It was reaffirmed that the multistakeholder format is a defining feature of the IGF, ensuring inclusiveness, democratic legitimacy, and balanced participation among governments, businesses, the technical community, academia, and civil society. In a context marked by tensions between multilateral and multistakeholder approaches, it is recommended to safeguard and strengthen this model.

Structure the pathway from outputs to impact ("outcome pathway").
It is recommended to accompany the outputs of main sessions and intersessional work with clear indications regarding target audiences, potential use contexts, and follow-up mechanisms, in alignment with the implementation of the Global Digital Compact and the WSIS+20 follow-up.

Strengthen links between the IGF and the UN system.
It is recommended to consolidate operational connections between the IGF and key UN entities working on digital, human rights, development, and capacity building, promoting regular exchanges and the use of IGF outputs in relevant processes (e.g., CSTD/ECOSOC, UN AI and digital initiatives, development and human rights programmes), while avoiding duplication and maximizing coherence.

Promote coherence among regulatory and policy approaches at the global level.
The debate highlighted increasing interaction among regulatory instruments, including within the European context (e.g., AI Act and Digital Services Act). The IGF should continue to serve as a platform for dialogue among different regulatory approaches, fostering interoperability and mutual understanding across legal systems.

Enhance the role of NRIs as implementation channels.
The importance of coordination between global and national levels emerged clearly. It is recommended to strengthen mechanisms linking the IGF with NRIs, enhancing their role not only in consultation but also in operational follow-up, evidence collection, and the testing of replicable solutions.

Integrate emerging priorities in digital governance.
In light of ongoing transformations—particularly in artificial intelligence, cybersecurity, and data governance—it is recommended that the IGF continue to provide a structured platform for discussion, ensuring an approach centered on human dignity, fundamental rights, and international cooperation.
Overall, these recommendations highlight the need for a strengthened, inclusive IGF, more closely interconnected with the UN system and major international platforms, and capable of exerting a more concrete impact on multilevel digital governance processes.

For the European Commission

In light of the issues that emerged during the discussions, the recommendations addressed to the European Commission are framed within the implementation of recent digital regulations and the need to ensure coherence, competitiveness, and the protection of rights in the process of technological transformation, also in relation to global digital governance dynamics.

Ensure coherent and harmonized implementation of the AI Act.
It is essential to guarantee uniform application of the European regulation, preserving the risk-based approach and its dual objective of fostering innovation while protecting fundamental rights. Strengthening coordination among national competent authorities and promoting shared interpretative guidelines is particularly important, especially in high-impact sectors and public administration applications.

Strengthen integration among European regulatory frameworks.
The debate highlighted increasing interaction between the AI Act and the Digital Services Act, particularly regarding transparency obligations and systemic risk management. It is recommended to promote an integrated approach across regulatory domains, avoiding fragmentation and ensuring regulatory interoperability for both public administrations and businesses.

Support European competitiveness in the global AI landscape.
In a context characterized by significant non-European investments and geopolitical dynamics, it is recommended to strengthen investment, research, and innovation policies in artificial intelligence, while ensuring alignment with European values of security, rights protection, and human centrality.

Promote high standards of security and digital resilience.
It was reiterated that secure AI cannot exist without robust cybersecurity measures. It is therefore recommended to consolidate European security standards and strengthen coordination among Member States in oversight and resilience of digital systems.

Invest in skills and AI literacy at the European level.
Skills were identified as a structural condition for digital transformation. It is recommended to strengthen European initiatives in training, upskilling, and reskilling, with particular attention to supporting SMEs and public administrations in the responsible adoption of AI.
Reinforce the EU's role in global digital governance.
The Commission is encouraged to continue promoting a European approach to digital governance based on openness, protection of fundamental rights, and the multistakeholder model, strengthening the EU's participation in global processes, particularly within the WSIS+20 framework and the implementation of the Global Digital Compact.

Foster links between European policies and multistakeholder initiatives.
It is important to strengthen connections between EU policies and multistakeholder initiatives, including national and regional Internet Governance Forums (NRIs), to enhance knowledge exchange and improve the territorial implementation of digital policies.
Overall, these recommendations point to the need for a coordinated and strategic European action capable of balancing innovation, security, fundamental rights, and competitiveness, in line with the regulatory and value-based framework highlighted during the 2025 edition.

For Businesses

In light of the evidence that emerged during the discussions, the recommendations addressed to the business sector are situated within a digital transformation that requires strategic awareness, structured governance, and investment in skills.

Integrate AI within a conscious corporate governance strategy.
AI adoption should not be treated as a standalone technological choice but embedded within an organizational model that incorporates accountability, transparency, and human oversight. Companies should develop internal governance mechanisms aligned with the European regulatory framework.

Address gaps in digital maturity.
A significant portion of enterprises has not yet completed cloud migration and still makes limited use of data and AI. It is recommended to invest in digital infrastructure and to leverage data as a strategic asset, in line with European 2030 objectives.

Adopt a value-oriented approach beyond short-term financial ROI.
AI should be considered a driver of competitiveness and resilience in the medium to long term, especially in a global context shaped by strong investments and geopolitical dynamics. Businesses are encouraged to assess AI's impact also in terms of organizational innovation, process quality, and sustainability.

Invest in structured training and AI literacy.
Skills are essential for a conscious and responsible use of AI. It is recommended to promote continuous training pathways and strengthen digital culture within organizations, avoiding fragmented or episodic approaches.

Mitigate risks associated with uninformed use of technologies.

The debate highlighted the risks of uncritical AI use, which may distort decision-making processes. Companies are encouraged to establish clear internal policies governing the use of generative tools, integrating data protection, security, and rights protection.

Strengthen security and system resilience.
Cybersecurity must be treated as a structural prerequisite for innovation processes. Companies should ensure high standards of reliability, security, and protection across their systems.

Enhance collaboration with universities and public administration.
Strengthening cooperation between businesses, academia, and public institutions is essential to foster innovation diffusion, skills development, and responsible AI adoption.
Overall, these recommendations encourage businesses to view artificial intelligence not only as a technological opportunity, but as a driver of organizational and cultural transformation, to be governed in a responsible and strategic manner aligned with the European regulatory framework.

For Universities

In light of the reflections developed during the 2025 edition, the recommendations addressed to universities are framed within the broader context of digital transformation and the evolution of artificial intelligence, which simultaneously impact teaching, research, and third mission activities.

Strengthen AI literacy as a transversal competence.
There is a clear need to promote a comprehensive understanding of artificial intelligence, encompassing not only technical aspects but also ethical, social, and legal implications. Universities are encouraged to integrate these competencies into curricula, fostering a critical approach to technology use.

Integrate technical and ethical education.
Awareness was identified as a prerequisite for responsible AI use. It is recommended to combine engineering and technical skills with legal, economic, and social perspectives, adopting a multidisciplinary approach consistent with the complexity of digital governance.

Address the risk of uncritical use of technologies.
The potential impact of generative AI on cognitive and critical capacities was highlighted. Universities should develop clear guidelines for AI use in teaching and research, promoting individual responsibility and academic integrity.

Support research and innovation in line with the European framework.
In a context of significant global investment in AI, universities play a key role in developing advanced skills and strengthening European competitiveness. It is recommended to promote research programmes and partnerships that combine technological innovation with rights protection, in line with the AI Act.

Strengthen technology transfer and collaboration with the productive system.

Universities should actively contribute to knowledge transfer and the development of innovative solutions, fostering collaboration with businesses and public administrations and supporting the dissemination of best practices in AI adoption.

Engage in multistakeholder governance models

The value of the multistakeholder model was reaffirmed as a reference framework for digital governance. Universities are encouraged to actively participate in consultation processes and forums, contributing scientific expertise and independent analysis.
Overall, these recommendations highlight the strategic role of universities in building widespread competencies, promoting a critical culture of innovation, and strengthening Europe's positioning in digital governance.

For Civil Society

In light of the reflections that emerged during the discussions, the recommendations addressed to civil society are framed within a digital transformation that requires informed participation, shared responsibility, and active safeguarding of fundamental rights.

Promote informed and conscious digital citizenship.

A strong need emerged to strengthen AI literacy as a civic competence, understood as the ability to comprehend the functioning, limitations, and ethical implications of artificial intelligence. Civil society is called upon to contribute to the dissemination of knowledge and critical tools, fostering a responsible use of digital technologies.

Counter disinformation and content manipulation.

The debate highlighted the risks associated with the creation or manipulation of content through AI systems, with potential impacts on public discourse and democratic processes. It is recommended to strengthen awareness-raising and monitoring initiatives, contributing to the protection of information quality and the transparency of digital ecosystems.

Support the multistakeholder model and participation in governance processes.

The multistakeholder approach was reaffirmed as a defining feature of Internet governance. Civil society is encouraged to actively participate in dialogue forums, contributing perspectives, expertise, and experience to the shaping of digital policies.

Safeguard fundamental rights.

The European framework on artificial intelligence is oriented toward the protection of rights, security, and human centrality. Civil society can play a key role in monitoring the implementation of regulations and promoting AI use aligned with principles of equity, inclusion, and accountability.

Foster social cohesion and digital inclusion.

It was noted that digital transformation can exacerbate cultural and territorial divides if not accompanied by inclusive policies. Civil society organizations are therefore encouraged to contribute to reducing the digital divide by supporting education, literacy initiatives, and equitable access to technologies.
Overall, these recommendations outline an active and proactive role for civil society in building an open, inclusive, and responsible digital ecosystem, grounded in participation, the

protection of rights, and cooperation among stakeholders within a multilevel governance framework.