ENCATC
The European network on cultural management and policy

Cultural Policy TRACKER

Governing Intelligence

www.encatc.org | ENCATC Cultural Policy Tracker

Issue N°13 | 2026
ISSN: 2959-2364

content

editorial

Artificial intelligence is rapidly transforming how knowledge is produced, how creative content circulates and how institutions make decisions. Yet the most important questions raised by this transformation are not technological alone. They concern authorship, responsibility, cultural diversity and the ways in which societies govern knowledge, creativity and cultural heritage.

The 13th issue of the ENCATC Cultural Policy Tracker examines the cultural and governance dimensions of responsible digital transformation. Across different legal, institutional and geographical contexts, the contributions in this edition ask a common question: what must remain human, participatory and publicly accountable as AI becomes more deeply embedded in cultural and social life?

Filippo Bagni and Luciana Lazzeretti explore this question through the European Union's regulatory framework. Their analysis of AI regulatory sandboxes considers how companies and public authorities can experiment together within controlled environments. These mechanisms aim to reduce regulatory uncertainty while supporting innovation, particularly among small and medium-sized enterprises, and give regulators direct insight into emerging technologies. At the same time, the authors remind us that experimentation requires clear safeguards, effective coordination and strong institutional capacity.

The question of participation becomes even more urgent in Mika (Jaeyun) Noh's contribution on Training Data Justice. Generative AI systems are built from vast quantities of cultural material, often collected without meaningful consent, attribution or

compensation. The article demonstrates that the governance of training data is inseparable from cultural sustainability. Communities must not only be consulted about the use of their cultural expressions; they must also have the capacity to influence decisions, retain cultural integrity and share in the value generated from their knowledge.

Elena Raevskikh and Giovanna Di Mauro examine one of the fundamental limits of automation: the distinction between information and judgement. AI can identify patterns, anticipate risks and organise vast quantities of data. It cannot, however, decide why one cultural site should be preserved over another, how competing public priorities should be reconciled, or what constitutes a legitimate course of action. These decisions depend on cultural context, collective memory, ethical responsibility and forms of tacit knowledge that cannot be fully codified.

Protecting digital cultural heritage is the focus of Emanuele Bellini's article on cyber humanities. As cultural heritage becomes increasingly digital, it is exposed not only to technical failure but also to cyberattacks, manipulation and new vulnerabilities that call for more integrated approaches to protection and resilience. Bellini proposes a transdisciplinary approach capable of bringing together humanities, cybersecurity and digital technologies to protect cultural assets across their full lifecycle.

Together, these four contributions suggest that responsible AI cannot be achieved through technical performance alone. It requires the protection of cultural rights, meaningful participation, resilient institutions and professionals able to work across

disciplinary boundaries. Most importantly, it requires recognition that culture provides the frameworks through which societies interpret information, evaluate consequences and decide what matters.

The task before cultural policymakers is therefore not to resist technological change, nor to accept it as inevitable. It is to shape the conditions under which innovation serves cultural diversity, democratic accountability and the public interest. Governing intelligence ultimately means recognising that technological progress and cultural values must advance together. The future of AI will depend on the collective capacity to shape it responsibly, inclusively and in the public interest.

Yours sincerely,

GiannaLia Cogliandro Beyens
ENCATC Secretary General

Regulation Meets Innovation in AI: The Role of Regulatory Sandboxes in the EU Digital Ecosystem

Filippo Bagni
Research fellow, CybeRights Research Centre;
Legal Officer, European Commission*

Luciana Lazzeretti
Emeritus Professor, previously a Full Professor,
of "Economics and Management"

1. Introduction

The debate on postmodern society's evolution towards a new digital society characterised by algorithmic dominance is intensifying. Some of these concerns are directly tied to the cybernetic nature of algorithms and the concept of the "black box society"[1]. There is also a growing demand for discussions about the ethics of algorithms in both private and public discourse[2], and jurists have also been active in highlighting issues related to the loss of protection for fundamental rights[3]. Furthermore, the digital economy plays a significant role in spreading fake news and propaganda, which has economic, political and cultural implications[4]. Artificial intelligence (AI), especially in its latest "generative" form, is a paradigmatic technology characterised by innovative and transformative capabilities that are pervasive and capable of rapidly changing not only products and services, but also entire sectors and society itself. While it offers significant opportunities, it also generates risks[5].

* Peer-reviewed article. The views and opinions expressed are those of the author only and do not reflect or represent any official policy or position of the European Commission.

[1] See F. Pasquale, *The black box society*, Cambridge, 2015.

[2] See L. Floridi, *The ethics of artificial intelligence. Principles, challenges, and opportunities,* Oxford, 2023.

[3] See H.W. Micklitz - O. Pollicino - A. Reichman - A. Simoncini - G. Sartor - G. De Gregorio (eds.), *Constitutional challenges in the algorithmic society*, Cambridge, 2021.

[4] See L. Lazzeretti, *The rise of algorithmic society and the strategic role of culture*, Cheltenham, 2023; S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, London, 2019.

[5] See F. Bagni, *Commento agli articoli 57 e 58*, in A. Mantelero – G. Resta – G.M. Riccio (a cura di), *Intelligenza artificiale. Commentario al Regolamento (UE) 2024/1689*, Milan, 2025.

The EU institutions have attempted to address these risks through a recent "wave" of regulations[6]. This EU regulatory approach, including the AI Act, is human-centred and aims to protect the rights of citizens and society. However, it also carries the risk of affecting the innovative capacity of EU companies operating in the global market, where approaches to AI differ greatly (such as the American and Chinese models)[7].

In this complex context, it is crucial to analyse the economic and legal aspects of this transformation together. One of the most debated issues among academics and EU regulators is the relationship between regulation and innovation in the context of AI technology applications. To this end, the EU Commission has invested heavily in the experimental tool of "regulatory sandboxes" in its new regulations (AI Act, Cyber Resilience Act, Interoperable Europe Act). These are normative experimental spaces in which companies and institutions situated in physical or virtual technological ecosystems interact to develop innovative processes for the ideation, development, and testing of responsible and compliant AI systems[8].

However, this evolving regulatory landscape poses challenges. The complexity and compliance burden of AI regulation can create barriers to innovation, particularly for start-ups and SMEs. Recognising this, EU policymakers have emphasised the need for mechanisms that strike a balance between regulation and innovation-friendly policies. The Draghi 2024 report and the EU Commission's new programme explicitly highlight the importance of

[6] During the first von der Leyen presidency (2019–2024), the EU experienced a significant acceleration in digital regulation. Over the past decade, the EU has developed a comprehensive and sophisticated body of law governing digital technologies, characterised by the rapid production of effective directives and regulations. The most heavily regulated areas include cybersecurity, covered by NIS2 (Directive (EU) 2022/2555), the EU Cybersecurity Act (Regulation (EU) 2019/881), and most recently the Cyber Resilience Act (Regulation (EU) 2024/2847); data protection, covered by the Data Governance Act (Regulation (EU) 2022/868) and the Data Act (Regulation (EU) 2023/2854); digital platforms, covered by the Digital Services Act (Regulation (EU) 2022/2065) and the Digital Markets Act (Regulation (EU) 2022/1925); and finally, AI, covered by the AI Act (Regulation (EU) 2024/1689).

[7] See E. Hine – L. Floridi, *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies, in AI and Society*, 2022, 1-2; C. Cath – S. Wachter – B. Mittelstadt – M. Taddeo – L. Floridi, *Artificial intelligence and the "good society": the US, EU, and UK approach, in Science and Engineering Ethics*, 24, 2018, 505 ff.

[8] See K. Yordanova - N. Bertels, Regulating AI: *Challenges and the Way Forward Through Regulatory sandboxes*, in H.S. Antunes et al. (eds.), *Multidisciplinary perspectives on artificial intelligence and the law*, Cham, 2024, 441 ff.; OECD, *Regulatory sandboxes in artificial intelligence*, Paris, 2023.

complementing regulation with policies that support AI-driven business growth. In this context, the EU digital ecosystem has a crucial role to play. This paper aims to explore the regulatory sandbox tool and its potential application in AI innovation, particularly within digital ecosystems characterised by the presence of SMEs. We will examine the contexts in which companies operate and how they can collaborate efficiently to strike a balance between regulation and innovation through co-participatory, multilevel governance.

The paper is organised as follows. After the introduction in the first section, the second section discusses the paradigmatic nature of AI technologies and their impact on businesses' innovation processes. It then introduces the concept of an entrepreneurial ecosystem, where innovation meets regulation. The third section discusses the "digital ecosystem" from economic and regulatory perspectives. First, we distinguish between two fundamental economic models: corporate and territorial frameworks. Secondly, we introduce the EU digital framework, defined by key policy initiatives implemented by EU legislators to support innovative enterprises. Finally, the fourth section analyses the regulatory sandbox as an innovative instrument for regulatory experimentation. It explores their core design features, and the EU legal definitions introduced in 2024, paying particular attention to the AI Act and the emerging secondary regulatory framework. Some concluding remarks highlight the paper's key contributions, particularly its integrated economic and legal perspective on the subject matter.

2. Artificial Intelligence and Ecosystems: Key Concepts

2.1. Artificial Intelligence as a Socio-Techno-Economic Paradigm

There are multiple definitions of AI[9], as well as numerous theories from various disciplines that have contributed to the emergence of "data science"[10]. However, even today, AI remains an umbrella term that encompasses a diverse range of computational technologies. Generally, AI

[9] See H. Gardner, *Frames of Mind: The Theory of Multiple Intelligences*, New York, 1983.

[10] See A. Agrawal – J. Gans – A. Goldfarb (eds.), *The Economics of Artificial Intelligence: An Agenda*, Chicago, 2019, 648 ff.

refers to the ability of machines to reproduce or implement operations that are typically associated with human cognitive functions.

Economists Furman and Seamans[11] describe AI as technologies with human-like intelligence, including machine learning, robotics, autonomous vehicles, computer vision, language processing, virtual agents and neural networks. MIT scholars Acemoglu and Restrepo[12] consider AI to be a "technology platform" that can be developed in both the service and production sectors. The EU Commission[13] states that AI-based systems may be software operating in the virtual world (e.g. voice assistants, image analysis software, search engines and voice and facial recognition systems) or integrated into hardware devices (e.g. industrial robots, self-driving cars, drones and IoT applications)[14]. This expands their scope and application across various industries.

Regardless of the adopted definition, it is undisputed that AI is the result of a long evolutionary process beginning with the discovery of computational theory and Turing's first computer in 1937 and culminating in the current "Summer of AI" phase[15], including its relationship with law[16]. Scholars in various scientific disciplines generally agree that AI is a disruptive innovation[17]. This has resulted in the obsolescence of many industries, products and professions, while simultaneously fostering the emergence of new ones. AI-driven technologies exhibit several defining characteristics, including transformative potential, transferability,

[11] See J. Furman – R. Seamans, *AI and the economy*, NBER Working Paper 24689, 2018..

[12] See D. Acemoglu – P.P. Restrepo, *The wrong kind of AI: Artificial intelligence and the future of labor demand, in Cambridge Journal of Regions, Economy and Society*, 13(1), 2020, 25 ff.

[13] See European Commission, *Artificial Intelligence for Europe*, Brussels, 2018.

[14] European Commission (2018). *Communication from the Commission to the EU Parliament, the EU Council, the Council, the EU Economic and Social Committee and the Committee of the Regions, available at eur-lex.europa.eu.*

[15] The "first real Summer of AI" can be pegged to 1956 at the famous Dartmouth University workshop when John Mc Carty coined the term. But in new millennium the summer of AI began in the first decade during the era of deep learning and big data.

[16] See T.B. Capon – M. Araszkiewicz – K. Ashley – A.Z. Wyner, *A history of AI and Law in 50 papers, in Artificial Intelligence and Law*, 20(3), 2012, 215 ff.

[17] See C.M. Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Boston, 1997.

pervasiveness, accessibility, speed and opacity. This is essentially an innovation that has generated a paradigmatic shift. Indeed, Kaplan[18] emphasised its socio-economic impact, and Von Hippel[19] highlighted the impact of mobile phones on social behaviour. Cristianini[20] consider the evolution of AI to be a "social machine". For these reasons, the seminal contributions of Freeman[21] and Carlota Perez[22] on the nature of techno-economic paradigms are applicable to the digital revolution in the same way as they are to the industrial revolutions triggered by the steam engine or electricity[23]. AI technologies present many important features, some of which are particularly relevant in this context, including transformative capacity, transferability, pervasiveness, accessibility, speed and opacity[24]. AI-related technologies have a strong transformative character in terms of their effects on innovation processes, both in terms of the evolution/transformation of the technologies themselves, which are changing and updating rapidly, and in terms of their impact on products and services, as well as on innovation processes, production/sales processes, production machinery and the tasks of workers. These technologies also have strong transmissibility and find applications at a multisectoral level, generating clusters of innovations in some cases. The sectors involved range from telecommunications and security to industry, education, management, finance, medicine and art, although the main topics remain in science and computer science. Generative AI plays a particularly strategic role as it evolves rapidly and uses machine learning algorithms trained on large datasets to create original content in various formats, including text, audio, images and video. This capability has transformative potential across industries, but it also raises significant legal and ethical challenges. Given the rapid development of these technologies and their widespread applications, there is an increasing urgency to implement regulatory measures that promote responsible innovation while ensuring market integrity and consumer protection.

[18] See J. Kaplan, *Artificial intelligence: what everyone needs to know*, Oxford, 2016.

[19] See E. Von Hippel, *Democratizing innovation*, Boston, 2005.

[20] See N. Cristianini – T. Scantamburlo, *On social machines for algorithmic regulation, in AI and Society*, 2020, 1 ff.

[21] See C. Freeman, *The economics of industrial innovation*, Harmondsworth, 1974.

[22] See C. Perez, *Technological revolutions and financial capital*, Cheltenham, 2002.

[23] A paradigm shifts when a scientific community changes its values, goals and methods: and it is perfect the case of AI according to the vision of the philosopher Thomas Kuhn in *The Structure of Scientific Revolutions*, Chicago, 1962.

[24] See D. Acemoglu – P.P. Restrepo, *The wrong kind of AI: Artificial intelligence and the future of labor demand*, cit., 25 ff.

2.2. The Entrepreneurial Ecosystem: Evolution of the Concept

The concept of an ecosystem in economic and managerial literature originated from ecological theory and was later adopted in studies of the evolution of economic systems, particularly those characterised by SMEs and business networks. Over the past few decades, the ecosystem framework has emerged as a key analytical tool for examining local economic systems, particularly in Europe. Over time, it has overlapped with various theoretical models, including Marshallian industrial districts, Porter's clusters, regional clusters, milieu innovators and regional innovation systems[25]. Today, the ecosystem framework is one of the most widely applied paradigms for analysing innovation dynamics in local economic development, focusing particularly on collaborative interactions between economic and non-economic actors.

Several definitions of ecosystems have been proposed in the literature, each highlighting different core dimensions, such as the roles of business, innovation, knowledge creation, and entrepreneurship. These elements have subsequently converged into the broader concept of the entrepreneurial ecosystem. Some scholars define business ecosystems as «the interconnectedness and dependency of organisations for mutual survival and effectiveness; the coexistence of a collaborative and competitive approach among organisations that share the same fate and resources»[26]. In the context of knowledge ecosystems, other scholars highlight a broader spectrum of social and public actors engaged in collaborative, symbiotic relationships that facilitate the exchange of tacit knowledge. The role of local research centres and universities as key enablers of knowledge creation and dissemination is emphasised[27].

[25] See R. Capello – P.P. Nijkamp, *Handbook of regional growth and development theories*, Cheltenham, 2022; G. Becattini – M. Bellandi – L. De Propris, *A handbook of industrial districts*, Cheltenham, 2009; M. Porter, Clusters and the new economics of competition, Boston, 1998.

[26] See M. Iansiti – R. Levien, *The Keystone Advantage What the New Dynamics of Business Ecosystems Mean for Strategy, Innovation and Sustainability*, Boston, 2004.

[27] See B. Clarysse – M. Wright – J. Bruneel – A. Mahajan, *Creating value in ecosystems: Crossing the chasm between knowledge and business ecosystems, in Research Policy*, 43, 2014, 1164 ff.; C.K. Prahalad, T*he fortune at the bottom of the pyramid*, Philadelphia, 2005.

The term "innovation ecosystem" has become popular in industry, academia, and government. It is used in corporate, national or regional contexts in idiosyncratic ways. Jackson[28] defines an innovation ecosystem as «the complex relationships formed between actors or entities whose functional goal is to enable technology development and innovation». However, the term is also used in several other contexts, such as the corporate innovation system, where the territorial dimension is emphasised as being useful for developing open innovation processes directly within regional and national innovation ecosystems, also known as RIS (Regional Innovation Systems), or city innovation ecosystems. A digital innovation ecosystem refers to case studies of digital online platforms such as Apple and Google, on which customers, users, and developers can build synergistic relationships and generate network externalities, thereby increasing the value of hardware and software innovations.

The concept of entrepreneurial ecosystems is now primarily used to describe environments that foster the creation of new ventures and start-ups, as well as the development of innovation processes. Emphasis is placed on ecosystems that drive digital technology advancements, including entrepreneurial digital ecosystems and digital platforms29.

In conclusion, although there is not yet a shared definition of an entrepreneurial ecosystem, it can be defined as «a set of interconnected entrepreneurial actors, institutions, organisations and processes that formally and informally come together to connect, mediate and govern performance within the local entrepreneurial environment»[30]. This includes all interdependent actors and factors that are coordinated to enable productive entrepreneurship within a particular territory[31].

[28] See B.D.J. Jackson, *What is an innovation ecosystem?*, Washington DC, 2011.

[29] See H. Rocha – D.B. Audretsch, *Entrepreneurial ecosystems, regional clusters, and industrial districts: Historical transformations or rhetorical devices?*, in *Journal of Technology Transfer*, 2022; M.G. Jacobides – C. Cennamo – A. Gawer, *Towards a theory of ecosystems, in Strategic Management Journal*, 39(8), 2018, 2255 ff.

[30] See C. Mason – R. *Brown, Entrepreneurial ecosystems and growth-oriented entrepreneurship*, Final Report to OECD, Paris, 2014.

[31] See E. Stam, *Entrepreneurial ecosystems and regional policy: a sympathetic critique, in European Planning Studies*, 23(9), 2015, 1759 ff.

3. The EU Digital Ecosystem: Economic and Regulatory Perspectives

3.1. The Economic Perspective

With the rise of globalisation and digitalisation in the new millennium, consumption patterns have evolved, and business models have undergone profound transformation. The emergence of platform capitalism has reshaped global value chains and redefined relationships between firms, encouraging the adoption of network-based models that blur organisational boundaries and make them more permeable. These platforms provide the structural framework that enables economic actors to interact and co-create value.

Broadly defined, a digital ecosystem — encompassing both corporate and territorial models — can be understood as an organisational structure, either physical or virtual, that operates within interconnected environments enabled by digital infrastructures, such as 5G networks, data centres and cloud computing. Within these ecosystems, various stakeholders collaborate, including economic players such as technology firms, startups, banks, business angels and venture capitalists; non-economic entities such as universities and research centres; and institutional stakeholders such as public authorities, regulatory agencies and regional governments, as well as users and consumers. These actors play a critical role in fostering the sustainable technological innovation that underpins digital transformation.

These systems first emerged within big tech companies such as Apple, Microsoft, Alphabet (Google), Amazon and Facebook (Meta), where they have primarily been studied through a corporate lens, particularly in the United States. Digital platform-based corporations have fostered the development of extensive and increasingly complex networked ecosystems composed of constellations of interdependent firms built around complementarities at local and global scales.

However, in Europe, digital ecosystems have largely adopted a territorial approach, reflecting the institutional and economic diversity among EU

member states. Often designed to integrate innovation-driven activities with entrepreneurial development (e.g. new ventures and startups), these ecosystems have also been leveraged as industrial policy instruments. They represent the natural evolution of the organisational models that shaped industrial capitalism throughout the 20th and early 21st centuries, such as industrial districts, clusters, and regional innovation systems (RIS). EU digital ecosystems are typically characterised by a high concentration of SMEs and business networks where cooperative strategies play a central role. Key factors such as tacit knowledge, embeddedness, trust and social capital serve as strategic drivers, reinforcing innovation and competitiveness within these ecosystems.

However, these models have faced significant challenges in terms of competitiveness, primarily due to a delay in technological transition compared to countries such as the United States, as well as the absence of major EU technological platforms. This has created competitive disadvantages, particularly for SMEs operating in AI-based sectors with globally integrated and linked value chains. Consequently, issues have arisen regarding the integration of territorial and corporate ecosystems, as well as the adaptation to differing regulatory frameworks.

There is an extensive body of literature on these topics, with a predominant focus on US-centric perspectives. Early studies distinguished between industry platforms, internal or company-specific platforms, and external or industry-wide platforms. More recent research has shifted towards digital platforms and digital ecosystems, with the two concepts becoming increasingly intertwined[32].

Parker et al.[33] define digital platforms as collections of digital resources, including services and content, which facilitate value-creating interactions between external producers and consumers. Hein et al.[34] build on this definition, describing a digital platform ecosystem as one in which a platform owner implements governance mechanisms to facilitate

[32] See M. Cusumano, *The Evolution of Research on Industry Platforms Academy of Management Discoveries*, in *Academy of Management Discoveries*, 2020

[33] See G.G. Parker – M.W. Van Alstyne – S.P. Choudary, *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*, New York, 2016.

value creation between themselves and a network of autonomous complementors and consumers. It is emphasised that digital platforms are built on digital infrastructures consisting of computing and network resources which enable various stakeholders to coordinate and fulfil their service and content needs.

Many platform scholars have shifted their focus to corporate success. Others have begun investigating the darker side of platform systems, introducing topics such as dominant positions, platform risks, and the potential for self-regulation within platforms[35]. One of the most debated issues is that of competition and regulation[36].

Another relevant topic is self-regulation[37]. From a historical perspective, both pre- and post-Internet, they suggest that combining self-regulation with credible threats of government regulation produces the best outcomes. Furthermore, effective self-regulation does not have to occur exclusively at the firm level. It requires collaboration between firms with similar business models to establish a set of jointly accepted rules or codes of conduct.

Finally, Bradford[38] addresses the prevalent belief that stricter regulation of the digital economy invariably stifles innovation and hinders technological progress. This view is vigorously advocated by the tech industry and has shaped public discourse in the United States, where lawmakers have also traditionally embraced it. However, the EU has chosen a different approach, regulating the digital economy with stringent data privacy, antitrust and content moderation regulations, among others, which are designed to shape the evolution of the tech economy towards EU values of digital rights and fairness.

[34] See A. Hein et al., *Digital platform ecosystems*, in *Electronic Markets*, 30, 2020, 87 ff.

[35] See A. Gawer, *Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age*, in *Innovation*, 24(1), 2022, 110 ff.

[36] See M.G. Jacobides – M. Bruncko – R. Langen, *Regulating Big Tech in Europe: Why, so what, and how understanding their business models and ecosystems can make a difference*, EvoltionLtd White Paper, 2020.

[37] See M.A. Cusumano – A. Gawer – D.B. Yoffie, *Can self-regulation save digital platforms?*, in *Industrial and Corporate Change*, 30(5), 2021, 1259 ff.

[38] See A. Bradford, *The false choice between digital regulation and innovation*, Oxford, 2024.

3.2. The Regulatory Perspective

The EU digital innovation ecosystem is a dynamic and rapidly evolving landscape. It is shaped by a variety of instruments that support businesses and public administrations in developing and deploying advanced digital technologies. Due to the scale and variety of initiatives across the 27 Member States, it is not yet possible to define the ecosystem with complete precision. Nevertheless, several core components can be clearly identified. Major funding programmers, most notably "Horizon Europe programme"[39] and the "Digital Europe programme"[40], provide strategic support for research, innovation and digital capacity building. These financial tools are complemented by specialised innovation infrastructures, such as the "European Digital Innovation Hubs" (EDIHs)[41], which help firms assess their digital maturity, experiment with new technologies and access technical expertise and advisory services. The ecosystem also includes "Testing and Experimentation Facilities" (TEFs)[42], which enable companies to trial AI-based technologies under real-world conditions, as well as "European Digital Infrastructure Consortium" (EDIC)[43], that coordinate large-scale, cross-border digital projects. Meanwhile, EU "Data Spaces" are emerging as

[39] Horizon Europe is the EU's research and innovation framework programme for the period 2021–2027, with an overall budget of approximately €95.5 billion. It offers extensive opportunities to support research and innovation projects in the digital field, particularly through Cluster 4 – Digital, Industry and Space, which promotes key technologies such as artificial intelligence, cybersecurity, cloud computing, and the Internet of Things, with the goal of strengthening Europe's technological sovereignty. See European Commission, *Horizon Europe – the EU Research and Innovation programme (2021–2027), available at research-and-innovation.ec.europa.eu.*

[40] The Digital Europe Programme is specifically dedicated to the digital transformation of Europe, with a budget of around €7.5 billion for 2021–2027. It aims to support the large-scale deployment of advanced digital technologies—including artificial intelligence, supercomputing, cybersecurity, digital skills—to enhance the EU's digital capacity and resilience. Cf. EU Commission, *Digital Europe Programme, available at digital-strategy.ec.europa.eu.*

[41] Further information available on the official websites: European Commission, *EU Digital Innovation Hubs, available at digital-strategy.ec.europa.eu/en/policies/edihs.*

[42] Further information available on the official websites: European Commission, *Testing and Experimentation Facilities (TEFs): Questions and answers, available at digital-strategy.ec.europa.eu;* European Commission, *EU Digital Innovation Hubs Network, available at EU-digital-innovation-hubs.ec.europa.eu.*

[43] Introduced under the Digital Decade Policy Programme 2030, EDICs are a new legal and collaborative instrument specifically designed to address a critical gap in the current digital ecosystem: the capacity to plan, fund, and manage large-scale, cross-border digital infrastructure projects in a coherent and strategic way. Unlike instruments such as TEFs and EDIHs - which support technology testing and

strategic assets, providing secure, interoperable environments for sharing sector-specific data across areas such as health, mobility, agriculture, energy and public administration. These data spaces foster trusted data flows and stimulate innovation across domains[44]. Most recently, "AI Factories" have been established to offer integrated environments for developing, training and scaling next-generation AI models, thereby lowering entry barriers for SMEs and start-ups[45].

This paper focuses specifically on TEFs, EDIHs and AI Factories, as their interaction is central to supporting technological experimentation and innovation. Their combined operation also provides a crucial foundation for understanding the function of AI regulatory sandboxes and how these infrastructures can reinforce the EU's broader approach to governing emerging technologies.

TEFs are advanced technical environments designed to help companies - especially SMEs - test innovative AI technologies in real-world conditions. These facilities, both physical and digital, allow companies to evaluate the performance of their AI-based solutions - such as intelligent software or robotics - before bringing them to market. TEFs provide access to state-

deployment at local or sectoral level – EDICs operate on a broader scale, overseeing the long-term deployment of shared EU infrastructures that surpass the capacity of individual Member States. Each EDIC is established by at least three Member States, with the approval of the European Commission, and becomes a legal entity tasked with delivering multi-country projects of strategic value—such as pan-EU data spaces, digital identity systems, smart city platforms, or blockchain infrastructures. Their governance is flexible, allowing Member States to define rules, funding mechanisms, and participation models suited to the specific needs of the initiative, ensuring both national ownership and EU-wide coherence. EDICs reflect Europe's growing need for joint ownership, interoperability, and sustainable management of digital infrastructure. Further information available on the official websites: European Commission, *EU Digital Infrastructure Consortium - EDIC, available at digital-strategy.ec.europa.eu/en/policies/edic.*

[44] By providing common rules, standards and governance frameworks, data spaces encourage collaboration between public and private organisations and support Europe's goal of digital sovereignty. They play a particularly important role in linking data-driven innovation to other elements of the ecosystem. More than 140 Data Spaces have been mapped across the EU, though only 31 are currently operational in 22 Member States. They are funded through the Digital Europe Programme and Horizon Europe, complemented by in-kind contributions from industry. Further information available at: *dataspaces-radar.org.*

[45] Further information available on the official websites: European Commission, *AI Factories*, available at *digital-strategy.ec.europa.eu*.

of-the-art infrastructure, technical expertise and hands-on support to integrate, validate and improve technologies in realistic environments. This enables companies to reduce innovation risks, accelerate development and improve the quality and reliability of their products. There are currently four active sector-specific TEFs in Europe - focusing on healthcare, manufacturing, agri-food and smart cities - spread across several Member States. Each TEF is structured as a network of centres – called nodes and satellites - that collaborate with each other and with businesses to provide coordinated and complementary services. While not every country hosts a physical node, all EU businesses can access TEF services through a single digital entry point for each sector. This model promotes not only technological innovation but also cross-border cooperation between Member States, fostering the sharing of knowledge and resources and the development of a truly integrated EU market for emerging technologies.

While TEFs focus primarily on the technological validation and experimentation of mature AI solutions, EDIHs provide broader, hands-on support for companies—especially SMEs—throughout their digital transformation journey. Acting as regional "one-stop shops", EDIHs help businesses assess their digital maturity and experiment with digital technologies, offering access to expertise, testing facilities, and advisory services. They also provide support in accessing funding, training workers, and integrating digital tools in a way that supports sustainable growth and innovation. Jointly funded by the European Commission and Member States under the Digital Europe programme, EDIHs form a pan-EU network of over 150 hubs[46], ensuring wide geographical coverage and enabling cross-border collaboration and knowledge exchange. Together, TEFs and EDIHs create a complementary system: TEFs support the technological readiness of advanced solutions, while EDIHs ensure that these innovations are effectively adopted and scaled across Europe's diverse industrial and public sectors.

[46] A full list and mapping are possible to find at the official website *EU-digital-innovation-hubs. ec.europa.eu.*

Finally, AI Factories are a new and strategic initiative within the EU digital ecosystem, designed to play a central role in empowering innovation among startups and SMEs in the field of AI. These facilities will serve as integrated hubs where computing power, high-quality data, technical expertise, and access to AI-optimised infrastructure converge—lowering the barriers that small players typically face when trying to develop and scale advanced AI solutions. AI Factories will give SMEs the chance to experiment with, develop and train the next generation of AI models, including generative AI. This will be achieved by bringing together supercomputing capacity, secure data spaces and dedicated AI development environments. This eliminates the need for substantial in-house infrastructure. The rollout of AI Factories has been prioritised as part of the 2024 "AI Innovation Package"[47]. AI Factories are also part of the wider digital ecosystem and are not designed as isolated projects, but as connective infrastructures that will link with TEFs and EDIHs, complementing their support to SMEs by providing the core computing and data resources needed to turn AI innovations into market-ready solutions[48].

4. Regulatory Sandboxes: Definition, Main Features, and Legal Framework

4.1. Definition of the Tool

The rapid pace of technological progress and the introduction of new products and services have created a new era of regulatory complexity[49]. The

[47] In a first wave, 7 AI Factories were established (Finland, Germany, Greece, Italy, Luxembourg, Spain and Sweden), followed by a second wave of 6 more (Austria, Bulgaria, France, Germany, Poland, and Slovenia). Further information available on the official websites: EU Commission, *AI Innovation Package, available at* digital-strategy.ec.europa.eu.

[48] Building on this, the "AI Continent Plan" announced the launch of five Gigafactories dedicated to developing and training the next generation of AI models. The AI Continent Plan particularly envisages the construction of five Gigafactories, each equipped with over one million advanced processors dedicated to training cutting-edge AI models. These facilities will focus on transformative sectors such as healthcare, biotechnology, manufacturing, robotics and scientific research. They will also be fully integrated into the EU digital ecosystem by collaborating with EuroHPC (the EU High-Performance Computing Joint Undertaking).

[49] See M. Weimer - L. Marin, *The Role of Law in Managing the Tension between Risk and Innovation: Introduction to the Special Issue on Regulating New and Emerging Technologies, in European Journal of Risk Regulation*, 3, 2016, 469 ff.

inherent fluidity of technological progress has tested the traditional rigidity of law and policymaking[50]. As a result, innovative regulatory approaches have been devised, some of which are referred to as "experimental lawmaking"[51]. These approaches include the addition of "experimental clauses"[52].

Within this broader context, regulatory sandboxes have gained prominence[53], providing the flexibility needed to meet the needs of the EU's evolving digital regulation strategy[54]: to balance regulatory oversight and innovation, while protecting fundamental rights and upholding fundamental legal principles.

The term "sandbox" traditionally evokes two images: one of playgrounds, where children can play without restrictions; and the other of computing, where it represents a safe testing environment that protects the system from malicious programs[55]. The addition of "regulatory" refers to a tool designed to test new services and products in a simulated regulatory environment.

[50] For an in deep analysis of the difficulties related to regulate innovation see L. Bennett Moses, *How to Think About Law, Regulation and Technology: Problems with 'Technology' as a Regulatory Target*, in *Law, Innovation & Technology*, 5(1), 2013, 1 ff.

[51] Some of the best doctrine has referred to these adaptive regulatory approaches as "experimental lawmaking". See S. Ranchordas, *Experimental lawmaking in the EU: Regulatory Sandboxes, in University of Groningen Faculty of Law Research Paper Series*, 12, 2021, 1 ff.

[52] For a detailed analysis see: M. Mousmouti, *Making Legislative Effectiveness an Operational Concept: Unfolding the Effectiveness Test as a Conceptual Tool for Lawmaking*, in *European Journal of Risk Regulation*, 9(3), 2018, 445 ff.; R. Van Gestel - G. Van Dick, *Better Regulation through Experimental Legislation*, in *European Public Law*, 17(3), 2011, 539 ff.

[53] The term "regulatory sandbox" first appeared formally at the EU level in the "Better Regulation Toolbox", among the possible tools for improving regulation: «Technological transformation, the emergence of new products, services, and business models can be quite challenging from a regulatory perspective. To enable firms to test innovations in a controlled real-world environment, under a specific plan developed and monitored by a competent authority, a relatively new policy instrument – a 'regulatory sandbox' – can be set up». See EU Commission, *Better Regulation Toolbox*, 2023, available at: *commission.europa.eu.*

[54] The expression "digital regulation" is not a legal one. It attempts to grasp the virtues of the EU legislators and regulators in creating a new environment for the EU market to grow by respecting fundamental rights and creating a balance between innovation and respect for the law. In its important scholarly work on the effects of EU law worldwide, Anu Bradford depicts digital regulation as a form of power that thoroughly influences the production and market of digital services and, as such, the digital economy. See A. Bradford, *The Brussels Effect: How the EU Rules the World*, Oxford, 2019.

[55] See K. Yordanova, *The shifting sand of regulatory sandboxes for AI*, in *KU Leuven CiTiP Blog*, 2019.

A regulatory sandbox is a controlled environment in which companies operating in regulated sectors, such as banking, finance and insurance, or in high-tech areas, such as AI systems and digital products, can test their innovative products and services for a limited period of time[56]. During this time, the testing is carried out in continuous communication with the supervisors responsible for ensuring the compliance of the innovative product/service before it enters the market, potentially benefiting from a simplified transitional regime. There is no one-size-fits-all sandbox model, and it depends on factors such as the technology used, the sector, the supervising authority, and others.

The main advantage of a regulatory sandbox lies in its ability to offer a safe space for experimentation - even allowing for potential mistakes - under the close supervision of regulators[57]. The goal is to develop an innovative product/service that complies with EU market rules by the end of the testing period. Specifically, regulatory sandboxes have a dual purpose: (a) promoting business learning, development and testing of innovations in a real-world environment; and (b) supporting regulatory learning by creating experimental regulatory frameworks to guide and support businesses in their innovative activities under the supervision of regulators.

The essence of the sandbox is based on a traditional win-win scenario. On the one hand, it facilitates market growth and development by enabling rather than hindering the introduction of technologically innovative products and services. At the same time, it ensures an appropriate level of consumer protection and competition through ongoing dialogue with regulators. While the company develops a product within an environment that provides guidance and, under certain conditions, possible regulatory exemptions, the regulator gains insight into the operator's activities and,

[56] See F. Bagni, *The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act*, in *Rivista Italiana di Informatica e Diritto*, 2, 2023, 201 ff.

[57] See A. Attrey - M. Lesher - C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, in *OECD Going Digital Toolkit Policy*, 2, 2020.

through continuous dialogue, acquires new technical expertise.

The regulatory sandbox model first emerged in the financial sector, where the combination of technological complexity and strict regulation provided an ideal environment for regulatory experimentation[58]. The United Kingdom (UK) played a pioneering role when, in 2016, the Financial Conduct Authority[59] (FCA) launched the world's first regulatory sandbox to facilitate fintech development and innovation[60]. This initiative quickly became a reference point for global regulatory practice, inspiring the creation of numerous sandbox schemes in jurisdictions worldwide[61]. Following its success in finance, the sandbox model has progressively been extended to other areas, including data protection[62] and, more recently, AI[63].

[58] See S. T. Omarova, *Technology v Technocracy: Fintech as a Regulatory Challenge, in Journal of Financial Regulation*, 6(1), 2020, 75 ff.

[59] For more information on FCA's Regulatory Sandbox, refer to *fca.org.uk/firms/innovation/ regulatory-sandbox.*

[60] See: T. A. Hemphill, *How State 'Regulatory Sandboxes' are Laboratories for Innovation*, 2021; J. R. Everhart, *The Fintech Sandbox: An Overview of Regulatory Sandbox Regimes, in Southern Journal of Business and Ethics*, 12, 2020, 64 ff.; J.J. Goo - H.J. Yeun, *The Impact of the Regulatory Sandbox on the Fintech Industry, with a Discussion on the Relation between Regulatory Sandboxes and Open Innovation*, in *Journal of Open Innovation: Technology, Market, and Complexity*, 6(2), 2020.

[61] Another significant example within the EU fintech domain is the regulatory sandbox established by Banca d'Italia (the Italian Central Bank). In particular, Banca d'Italia has developed a comprehensive experimentation framework based on three complementary pillars: (1) the Fintech Channel, consisting of an Innovation Hub created in 2017 to provide regulatory support to firms; (2) the Milano Hub, established in 2020 as a research-oriented space dedicated to the development phase of innovative projects; and (3) the regulatory sandbox proper, introduced in 2021.

[62] In this area, the role of national data protection authorities (DPAs) has been pivotal. Two particularly relevant examples come from the United Kingdom and Norway. In the UK, the Information Commissioner's Office (ICO) has set up a regulatory sandbox centred on personal data protection, exploring emerging technologies such as voice biometrics and facial recognition. In 2020, the Norwegian Data Protection Authority (Datatilsynet) launched a regulatory sandbox with a specific focus on the intersection of privacy and artificial intelligence. Initially introduced in 2021 as a two-year pilot under the national AI strategy, the sandbox aimed to foster privacy-friendly innovation and digitalisation.

[63] Two particularly relevant examples in this area are the CNIL Sandbox in France and the UK's AI Airlock. The French initiative, developed by the Commission Nationale de l'Informatique et des Libertés (CNIL), offers a sector-specific sandbox dedicated to AI applications in public administration. It provides a structured environment for collaborative regulatory experimentation and offers bespoke legal and technical guidance to public and private organisations looking to develop AI systems that comply with data protection and privacy requirements. The UK's Medicines and Healthcare Products Regulatory Agency (MHRA) launched AI Airlock in 2024. It is the UK's first sandbox dedicated to AI as a medical device (AIaMD) and addresses the regulatory challenges arising from the increasing use of AI in clinical settings.

4.2. Core Elements of Regulatory Sandboxing

Although the concept of regulatory sandboxes varies widely, certain common elements can be identified[64]. These common elements provide a clearer framework for understanding how sandboxes work and what conditions need to be met for their successful implementation[65].

First and foremost, regulatory sandboxes are designed for innovative products or services that are not yet available on the market. These offerings typically involve new technologies, business models or applications that do not fit neatly into existing regulatory frameworks[66].

Secondly, the product or service should demonstrate a social added value for consumers or society. This added value can include economic efficiency, increased accessibility, or contributions to broader public policy goals - such as financial inclusion, environmental sustainability, or digital transformation.

Thirdly, the product or service must be mature enough to be tested. This means that it must not be at the idea stage, but also not so mature that meaningful changes would be impossible during the testing period. It should be ready for market-like conditions, but still adaptable based on feedback.

Fourthly, the proposed activity must be commercially viable throughout the sandbox period. Participating companies must demonstrate that they have the financial capacity to carry out the test without risking business failure due to lack of resources. Economic sustainability is essential to ensure the continuity and reliability of the experimental process.

[64] For a detailed analysis see F. Bagni, *Regulatory sandboxes as a bridge between AI and cybersecurity: Exploring the interplay between the ai act and the cyber resilience act*, in F. Bagni – F. Seferi (eds.), *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders*, Florence, 2025, 54 ff.

[65] For a proper overview of the selection criteria, such as the innovative character of the project, public interest, alignment with broader policy objectives, project maturity, consumer safeguards, identification of regulatory barriers, time limits, specific authority mandates, the need for testing and increased legal certainty, please refer to the following studies and reports: EU Commission, *Commission Staff Working Document, Regulatory learning in the EU, Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy*, 2023, available at *data.consilium.europa.eu.*

[66] The degree of innovativeness of the solution is the most frequent criterion emerging from Seferi comparative analysis. For a detailed analysis see F. Seferi, *A working experimentation model for cyber resilience regulatory sandboxes, in Joint National Conference on Cybersecurity*, 1(3926), 2025.

Finally, for the sandbox to function effectively, it is crucial to identify the applicable legal framework and the regulatory barriers that the innovation may face. This includes clarifying the specific legislation against which the product or service will be tested, as well as identifying the competent authority responsible for supervising the experimentation and providing regulatory guidance.

In addition, to ensure the success of the experimentation process, a number of parameters need to be clearly defined from the outset. Legal predictability is essential for participating companies, and the boundaries and conditions of the sandbox should be defined in advance. Ideally, this should be done through legislation, regulatory guidance or memoranda of understanding with market surveillance authorities. Key parameters to be defined include: applicable legislation, eligible sectors, planned exemptions, rules for participation and selection, duration of the sandbox and conditions for exiting the scheme. These elements are fundamental for measuring results and assessing the impact of the sandbox.

Furthermore, appropriate safeguards must be put in place in a controlled environment to mitigate potential risks, particularly if testing is conducted in real-world conditions. For example, testing autonomous vehicles requires specific safety protocols to protect participants and the public[67].

Participation in regulatory sandboxes is generally subject to approval, supervision and evaluation by the competent authority. Access is often limited to a select number of participants during predefined application windows. Authorities typically invite interested operators to submit proposals, which are then evaluated through a structured selection process, including interviews and due diligence. Only after this process are projects formally admitted to the sandbox and allowed to begin testing under the agreed conditions.

[67] For a contribution emphasising the importance of safeguards in sandbox testing, particularly in the field of autonomous vehicles, see R. Von Thiessen, *Learnings from the AI sandbox in Zurich: A practical perspective*, in F. Bagni – F. Seferi (eds.), *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders*, cit., 177 ff.

For a long time, there was no precise institutional definition of regulatory sandboxes[68]. This absence is significant, as it shows that, despite the widespread use of sandbox-like instruments in various EU Member States, EU legislators had not yet formally conceptualised them. This changed in 2024 when three major EU regulations introduced explicit legal definitions, signalling a clear political and regulatory decision to invest in sandbox mechanisms in the context of the recent digital regulatory "wave".

Specifically, the Artificial Intelligence Act (Regulation (EU) 2024/1689) defines "AI regulatory sandboxes" in art. 3(1)(55); the Interoperable Europe Act (Regulation (EU) 2024/903) defines "interoperability regulatory sandboxes" in art. 2(1)(14); and the Cyber Resilience Act (Regulation (EU) 2024/2847) refers to "cyber resilience regulatory sandboxes" in art. 33(2)[69]. These provisions establish a clear and explicit legal basis for sandbox mechanisms at the EU level for the first time, providing a direct and binding framework across all Member States.

Although a detailed analysis of the sandbox regimes under each of these regulations is beyond the scope of this section, three observations are particularly relevant.

Firstly, the definitions provided in the AI Act, the Interoperable Europe Act and the Cyber Resilience Act broadly reflect the core features outlined above. This convergence enables the formulation of a general operational definition: a regulatory sandbox is a controlled environment established by a competent authority that enables public or private entities to develop, test and validate innovative solutions under regulatory supervision for a limited period and, where appropriate, in real-world conditions[70]. For the first time, therefore, a

[68] The Better Regulation Toolbox also recognises the lack of clarity surrounding the concept of regulatory sandboxes: «Although no commonly agreed definition exists, regulatory sandboxes can be broadly described as schemes enabling producers to test innovations in a controlled real-world environment, under a specific plan developed and monitored by a competent authority» (at 131).

[69] For the sake of completeness, it should be noted that a fourth regulation — the Net-Zero Industry Act (NZIA, Regulation (EU) 2024/1735) — was adopted in 2024. This introduces "net-zero regulatory sandboxes", which are defined as controlled real-world environments in which undertakings can test innovative net-zero technologies. These are developed and monitored by a competent authority (Arts. 26–27).

[70] The real-world testing enables more accurate, context-sensitive and practically relevant experimentation. However, it also introduces additional risks, particularly when real personal data or

common conceptualisation of the instrument begins to emerge at EU level.

Secondly, although key secondary legislation in the form of implementing acts is envisaged under both the AI Act and the Interoperable Europe Act, the Cyber Resilience Act does not include an equivalent provision. These implementing acts are expected to play a crucial role in defining the operational parameters of regulatory sandboxes, including the criteria for eligibility, the procedural requirements and the supervisory arrangements. Thirdly, the distinguishing feature of the AI Act is that it requires the creation of regulatory sandboxes at a national level; under the other two regulations, this remains optional. For this reason, the following section focuses specifically on the AI Act's regulatory sandbox provisions, as this framework will likely influence the future design and implementation of sandbox mechanisms within the European digital ecosystem.

4.3. AI Regulatory Sandboxes under the AI Act and Their Integration into the EU Digital Ecosystem

Due to the complexity of the regulatory framework, the aim of this section is not to provide an exhaustive analysis of the AI Act's sandbox regime[71]. Instead, it highlights several key elements that are particularly relevant when considering regulatory sandboxes as part of the wider European digital ecosystem.

high-impact scenarios are involved. To mitigate these risks, for example, the AI Act requires robust oversight by the relevant authority, the adoption of a specific "real-world testing plan" (see art. 3(1)(53)), and the implementation of appropriate safeguards to protect fundamental rights, health, and safety (see art. 57(4)).

[71] The AI Act expressly recognises regulatory sandboxes as instruments for fostering innovation (Chapter VI), dedicating arts. 57 and 58 to defining their objectives, structure, and operation. According to art. 57, each Member State must establish at least one fully operational national AI sandbox by August 2026. This marks a shift from fragmented, voluntary experimentation to a mandatory, harmonised EU-wide framework. Sandboxes are intended to enhance legal certainty, support the exchange of best practices, encourage innovation — particularly among SMEs and start-ups, who can participate free of charge — and facilitate structured regulatory learning. At the end of each experimentation cycle, the relevant authorities must issue an exit report and, where requested, additional documentation. While this does not create any presumption of conformity, it must be given due consideration by notified bodies and market surveillance authorities. Art. 58, in turn, assigns the EU Commission a central role in shaping the practical functioning of sandboxes through one or more implementing acts. These acts — still pending at the time of writing — will be decisive in ensuring a coherent and harmonised approach across the Union. They will define the operational architecture of national sandboxes in detail and ultimately influence their capacity to function as effective instruments of adaptive, collaborative, and forward-looking regulatory governance.

As mentioned previously, the AI Act is the only EU regulation that obliges Member States to set up AI regulatory sandboxes at a national level (art. 57(1))[72]. Consequently, a comprehensive network of AI regulatory sandboxes is expected to emerge across Member States in the near future. While this will significantly expand the European digital ecosystem, it will also create substantial challenges in terms of coordination, governance and operational consistency.

One of the most significant coordination challenges concerns the institutional dimension. Art. 57(10) of the AI Act, supported by recital 139, stipulates that national data protection authorities (DPAs) must be involved in operating and supervising AI sandboxes where personal data processing is concerned. Furthermore, art. 59 of the AI Act regulates the processing of personal data in the public interest within sandbox environments[73]. These provisions emphasise the importance of effective coordination between the relevant authorities, reinforcing the multi-authority nature of sandbox governance. The operational parameters of the sandboxes will be defined through one or more implementing acts adopted by the European Commission under art. 58(1). These acts are expected to address three key areas: (i) eligibility and selection criteria (art. 58(1)(a))[74]; (ii) procedural rules (art. 58(1)(b))[75]; (iii) and terms and conditions for participation (art. 58(1) (c)).

At the time of writing, the final version of the Implementing Act had not yet been adopted. However, a draft was published in December 2025[76].

[72] The core mandate of art. 57(1) is that each Member State shall establish at least one national regulatory sandbox for AI and ensure that it is fully operational within 24 months of the entry into force of the Regulation. The essential requirement is that, within this timeframe, each Member State guarantees the existence of at least one functional and accessible sandbox, providing market participants with a dedicated space to test their AI systems before placing them on the market.

[73] For an interesting focus on art. 59 of the AI Act and, more generally, on data protection aspects related to the AI Act and sandboxes, please refer to D. Baldini, *Legislative intersection perspectives on regulatory sandboxes: Navigating the interplay between the AI Act and the GDPR*, in F. Bagni – F. Seferi (eds.), *Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders*, cit., 70 ff.

[74] These rules will define who can apply to participate in a sandbox and how applications are to be evaluated. Eligibility refers to the general requirements that applicants must meet, while selection criteria relate to the qualitative indicators used to select applicants.

[75] These include the full procedural lifecycle of sandbox participation, from application and acceptance to monitoring, reporting and exit.

[76] See Commission Implementing Regulation (EU) .../... laying down rules for the application of Regulation (EU) 2024/1689 of the European Parliament and of the Council as regards the establishment, development, implementation, operation and supervision of AI regulatory sandboxes, draft text available at *digitalstrategy.ec.europa.eu/en/consultations.*

Despite expectations of a detailed and prescriptive framework, the draft is relatively concise, consisting of 25 recitals and 10 articles. Nevertheless, several important elements can already be identified.

Recital 5 clarifies that, in order to comply with the AI Act, each Member State must establish at least one "horizontal" national AI regulatory sandbox that is open to experimentation with any AI system that meets the general eligibility criteria set out in the Regulation.

Regarding participant eligibility and project selection — arguably one of the most legally significant aspect of the entire framework — recital 13 emphasises the need to consider regulatory and practical challenges, the maturity and competitiveness of the AI system, and the potential for regulatory learning to be scaled up. Notably, the draft adopts a nuanced understanding of "innovation", recognising that AI systems already on the market may qualify for sandbox participation if they are deployed in a new or significantly different context. Recital 13 should be read in conjunction with art. 3 of the same Act, which provides further specifications of the eligibility requirements (art. 3(2)) and the selection criteria (art. 3(3)). The references to scalability of regulatory learning, contribution to the public interest, maturity, economic viability and innovative character of the system are particularly relevant.

Another important point is the clear acknowledgement of the need to integrate AI regulatory sandboxes into the wider European digital ecosystem. Recital 16 and art. 4(5) of the draft Implementing Act emphasise the importance of connecting sandboxes to other key infrastructures such as TEFs, EDIHs and AI Factories. This approach is consistent with art. 57(4) of the AI Act, which anticipates the development of a coordinated, multi-level sandbox ecosystem throughout the EU[77]. The AI Act also requires structured coordination between national authorities, the European AI Office[78] (art. 64)

[77] This framework includes a mandatory sandbox in each Member State, with the possibility for additional initiatives at regional or local level, as well as a dedicated data protection sandbox under the supervision of the European Data Protection Supervisor (EDPS).

[78] It is established within the Directorate-General for Communication Networks, Content and Technology (DG CNECT) in the European Commission. The AI Office is the office in charge of supervise and enforce the AI Act requirements on general purpose AI models and AI systems across the 27 EU Member States.

and the European Artificial Intelligence Board (art. 65), to ensure coherence, transparency and harmonised implementation across Member States[79].

This systemic perspective makes clear that AI regulatory sandboxes should not be viewed as standalone instruments. Instead, they are part of an interconnected landscape alongside TEFs, which validate emerging technologies, EDIHs, which support SMEs in their digital transformation, and AI Factories, which provide the infrastructure needed to develop advanced AI systems. In this architecture, regulatory sandboxes serve as bridges, connecting innovation and regulation and providing entry points for companies, particularly SMEs and start-ups, into the broader digital support system. By integrating sandboxes into this value chain, EU regulators are seeking to create a coordinated pathway that supports companies from the earliest stages of product development through to regulatory alignment and full market deployment. However, the effectiveness of this model depends on all components being properly connected and mutually reinforcing, a condition that remains to be demonstrated in practice.

5. Concluding Remarks

This contribution examined the relationship between regulation and innovation within the evolving landscape of EU digital ecosystems. It has emphasised the paradigm-shifting nature of the ongoing technological transformation and the significant influence of the economic and institutional contexts in which innovation occurs. The analysis reveals that the EU is simultaneously presented with significant development opportunities and substantial systemic risks. These arise in an environment characterised by accelerating technological change, increasingly fragmented economic ecosystems, growing complexity in global value chains and an ever-expanding regulatory framework.

The EU brings together profoundly heterogeneous realities: large global technology firms embedded in extensive digital corporate ecosystems, and

[79] Such a complex structure requires efficient coordination at the European level. Art. 57 emphasises the importance of cross-border collaboration between national authorities (par. 13), especially within the context of the Board (para. 14) and enables them to request assistance and advice from the AI Office (para. 15).

territorial industrial systems composed of networks of small and medium-sized enterprises, often organised into clusters or technological districts. A third dimension must be added to this picture: the EU digital ecosystem, consisting of infrastructures, programmes, and multilevel governance mechanisms.

This inevitably produces tensions. Businesses must balance the demands of global markets with the obligations imposed by EU regulation. They also face rising compliance costs and the risk of competitive asymmetries widening with large technology companies. These challenges are intensified by Europe's recent "regulatory wave", which has resulted in a complex body of legislation. While these measures are crucial for safeguarding citizens, fundamental rights and fair competition, they may also result in overlaps, inconsistent implementation and coordination issues among regulatory authorities, potentially impacting SMEs with legal uncertainty and additional barriers to innovation.

Against this backdrop, regulatory sandboxes have emerged as a potentially pivotal mechanism for bridging the gap between technological innovation and regulatory oversight. By providing a controlled environment in which firms and authorities can experiment together with emerging technologies, sandboxes offer a practical way to reconcile technological dynamism with regulatory safeguards. From an economic perspective, they can reduce compliance costs, facilitate market access for SMEs and start-ups, and mitigate competitive imbalances with Big Tech. Institutionally, they promote regulatory learning and investment, enabling authorities to gain detailed, practical knowledge of new technologies — insight that conventional regulatory instruments rarely provide.

Sandboxes can also help to manage the complexity of digital ecosystems. Such ecosystems are highly interconnected, as are the value chains of local and global firms, as well as the legal frameworks that govern economic and social life. This interconnectedness generates two main categories of risk. First, infra-ecosystem risks stem from the need to reconcile the bottom-up economic logic of enterprises with the top-down constraints of regulatory ecosystems. Inter-ecosystem risks arise when SMEs must comply with both global market rules, which are often linked to participation in global value chains, and the requirements established by EU regulators. SMEs must assess the economic and competitive consequences of this overlapping regulatory landscape, particularly given competitive pressure from Big Tech and the risk of structural asymmetries.

The paper's suggestion of using regulatory sandboxes is precisely intended to address this complexity. By enabling companies to innovate within regulatory boundaries while pursuing competitive advantages and reducing exposure to competitive asymmetry through participatory and operational experimentation, sandboxes facilitate innovation. At the same time, they allow regulators to learn directly from the challenges firms encounter and address these through structured dialogue. Thus, sandboxes support a more participatory, efficient and sustainable governance model based on cooperation between institutions and enterprises.

From a regulatory perspective, the sandbox model reveals its most innovative dimension. Traditional regulation usually follows a top-down approach: rules are established first and the industry must adapt. In contrast, the sandbox model introduces an important inversion. Rather than merely applying preexisting rules, regulators and regulated entities can collaboratively design regulatory solutions through structured, hands-on experimentation to some extent. In the field of emerging technologies, law becomes an iterative, dialogic process shaped not only by abstract principles, but also by concrete operational evidence. In this sense, the sandbox functions as a "laboratory" for norm-making, where experimentation can inform future regulatory standards, guidance, and supervisory strategies. This evolution reflects a broader conceptual shift towards viewing regulation as an adaptive, relational, and evidence-based activity. The widening gap between traditional regulatory methods and rapidly advancing technologies cannot be overcome with static rules alone. There is an increasing need for instruments that evolve alongside the technologies they aim to govern.

The sandbox model is not without limitations. The AI Act's sandbox regime — also in light of the draft Implementing Act — highlights this. Key aspects, including eligibility criteria, selection procedures and operational arrangements, still need to be specified and tested in practice. The mandatory involvement of Data Protection Authorities in some cases introduces a coordination requirement that cannot be taken for granted. More broadly, the absence of unified governance structures, the risk of forum shopping across Member States, the possibility of regulatory capture or ethics washing (Francis, 2025; Zarra, 2025), and persistent asymmetries in technical expertise demonstrate that sandboxes are not a universal solution. They require substantial resources, methodological

rigour, clear objectives, and robust institutional capabilities, as well as a genuine commitment to sound sandbox design from all parties involved. If applied in the wrong context or with insufficient safeguards, a sandbox risks becoming, metaphorically, "quicksand". Therefore, careful assessment and clear criteria are essential in determining what should be subject to experimentation and under what conditions.

Nevertheless, regulatory sandboxes are one of the most ambitious attempts to balance technological innovation with legal protection — two objectives at the heart of Europe's strategic positioning. Their long-term effectiveness depends on their implementation, but their underlying rationale closely aligns with the EU's commitment to fostering innovation and becoming a global leader in developing safe, trustworthy, and value-driven artificial intelligence.

As mentioned previously, the AI Act mandates that each Member State establish at least one national AI sandbox by August 2026, though company participation remains voluntary. Therefore, it will be crucial for EU regulators to calibrate the model so that it is both effective and attractive without distorting competition. The success of this balancing exercise will ultimately determine whether regulatory sandboxes evolve into a stable instrument of co-regulation and adaptive governance within the EU digital ecosystem.

Publication context and acknowledgements
This article was first published in Rivista del diritto e dei media, Special Issue III/2026:
https://www.rivistadidirittodeimedia.it/rivista/regulation-meets-innovation-in-ai-the-role-of-regulatory-sandboxes-in-the-eu-digital-ecosystem/

AUTHORS

Filippo Bagni is a lawyer and researcher specialising in the regulation of the digital ecosystem, with a particular focus on artificial intelligence and cybersecurity. He is a Research Fellow at the CybeRights Research Centre in Florence, and he was awarded a PhD by the IMT School for Advanced Studies in Lucca as part of the Italian National PhD Programme in AI & Cybersecurity. He also works as a Legal Officer at the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT) in Brussels. His work sits at the intersection of law, economics, and technology, reflecting a genuinely interdisciplinary approach to some of the most pressing governance challenges of the digital age. He is the author of numerous publications on the law of new technologies and has recently published his first book, Sandboxing Innovation: Designing Regulatory Sandboxes for AI and Cybersecurity (Wolters Kluwer Italia).

Luciana Lazzeretti is an Emeritus Professor, previously a Full Professor, of "Economics and Management" at the Department of Economics and Management at the University of Florence. She currently teaches "Economics and Management of Sectors and Local Systems" on the Master's degree programme in Economic Science. Throughout her career, she has conducted extensive research and teaching activities in Italy and internationally, particularly in Europe, the USA, Canada, Brazil and Japan.

In the first decade of her career, she developed a line of research focusing on the processes of cultural districtalisation in art cities, primarily within the context of studies on the economics of culture and creativity. She later devoted herself to studying cultural organisations, cultural and creative industries, and cities and regions. Professor Lazzeretti has also dealt with regional policies supporting innovation and technology transfer, SME networks for innovation and technology transfer, and the evaluation of innovative projects. She has also studied the resilience of local systems following external shocks, including those caused by natural disasters, and analysed the economic complexity using relatedness tools. Recently, she initiated a strand of studies on the relationship between artificial intelligence and culture. She is the author of over 250 scientific publications and has been selected as one of Elsevier's Top Cited Scientists for the past three years.

Training Data Justice: Cultural Sustainability in the Age of Generative AI

Mika (Jaeyun) Noh
Founder & Executive Director, AI Culture Lab; Co-Founder & Chair, AI Art Forum, National Assembly of Korea

What is the issue

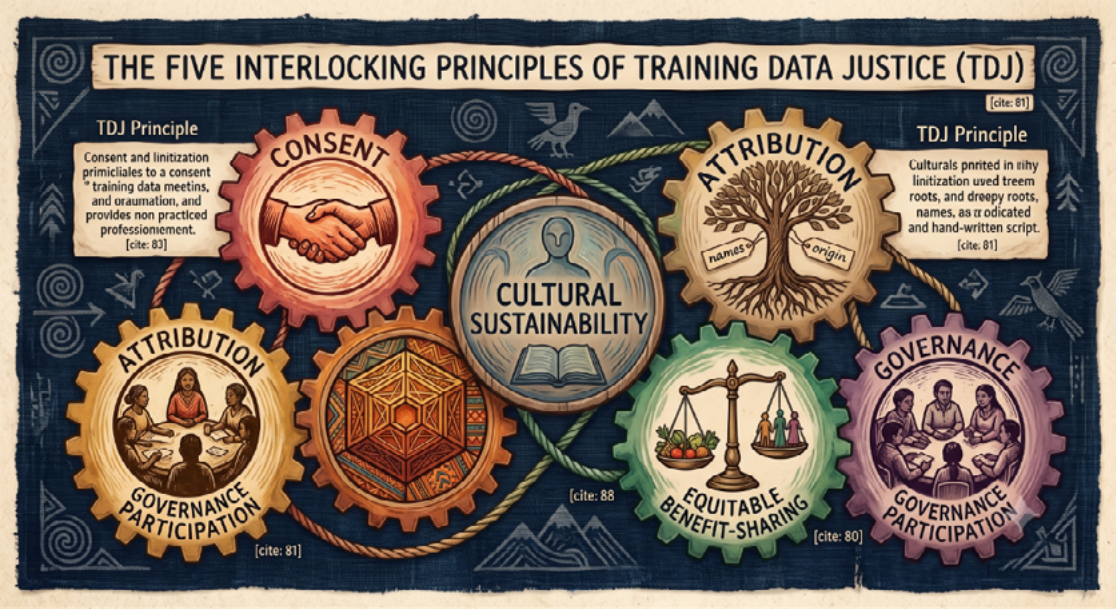
Generative AI systems are trained on vast corpora of text, image, and audio data, much of it scraped from the internet without the consent, attribution, or compensation of the cultural communities whose heritage, languages, and artistic traditions it represents. This is not a peripheral technical footnote. It is a sustainability issue in the fullest sense of the term: cultural sustainability depends on communities retaining the capacity to transmit, control, and benefit from their own knowledge across generations, and that capacity is being quietly eroded by the data practices underpinning today's AI economy.

Training Data Justice (TDJ) is a governance framework developed to address this gap. It treats training data not as a neutral input to be optimised for model performance, but as a matter of cultural rights, democratic accountability, and intergenerational equity. TDJ rests on five interlocking principles:

- **Consent —** communities must give genuine, informed consent before their cultural expression is used to train AI systems, not consent assumed from public availability or buried in platform terms of service.
- **Attribution —** when training data includes identifiable cultural material, authorship and community origin must remain traceable and publicly accountable.
- **Cultural integrity —** datasets must preserve, rather than flatten or decontextualise, the meaning embedded in cultural practice.

- **Equitable benefit-sharing —** economic and reputational value generated by AI systems trained on community data must be returned to the communities that produced it.

- **Governance participation —** affected communities must hold real decision rights over the systems that govern their cultural data, not merely be consulted after key design choices are fixed.



Why it is relevant

Cultural sustainability is conventionally framed around the preservation of heritage sites, languages, and traditional practices against the pressures of urbanisation, climate change, or economic precarity. Generative AI introduces a new and faster-moving pressure: the large-scale, often non-consensual extraction of cultural material into training datasets that then generate synthetic outputs at a speed and volume no human creative economy can match.

This matters for the cultural and creative sectors for at least three reasons.

- **Training data functions as cultural infrastructure.** The aesthetic norms, languages, and historical narratives a model can represent are determined by what it was trained on, and what it was trained

on is determined by whose digital archives were accessible, well-documented, and unprotected. Communities with strong digitisation but weak data governance are paradoxically more exposed to extraction than those with little digital presence at all.

- **The imbalance compounds existing global inequalities.** Major foundation models are trained disproportionately on English-language, Western-platform content, while labelling and content-moderation labour, much of which involves processing the most sensitive cultural and emotional material, is frequently outsourced to lower-waged workers in the Global South.
- **Without intervention, generative AI risks cultural homogenisation.** Outputs trained predominantly on dominant-culture data tend to reproduce dominant-culture aesthetics and narratives even when prompted in other cultural registers, narrowing rather than expanding the diversity of cultural expression in circulation.

What are the challenges

- **Scale versus consent —** foundation models are trained on datasets of a size that makes individual or community-level consent practically difficult to obtain retroactively, and few mechanisms yet exist for prospective, opt-in cultural data collection at comparable scale.
- **Jurisdictional fragmentation —** copyright, data protection, and cultural heritage law operate under different legal logics and national jurisdictions, while AI training pipelines operate transnationally, creating significant gaps in enforcement.
- **The attribution problem —** once cultural material has been absorbed into a trained model's weights, tracing a specific output back to specific source material is technically difficult, undermining both attribution and benefit-sharing mechanisms.
- **Resourcing asymmetry —** the institutions best placed to negotiate data governance terms with AI developers, such as well-resourced museums and major rights-holders, are rarely the same communities most exposed to extraction.

- **The normative-to-operational gap —** international ethics frameworks, including UNESCO's Recommendation on the Ethics of Artificial Intelligence, articulate strong cultural data principles, but few have been translated into deployable mechanisms cultural organisations can actually implement.

What are the possible solutions / open questions

Several governance mechanisms are emerging as practical responses, though none yet operates at the scale the problem requires.

Cultural data trusts offer one model: a legal and institutional structure through which a community collectively governs how its cultural data is licensed, used, and compensated, rather than leaving these decisions to individual creators negotiating alone against large platforms. Fieldwork developing such a trust with fifty artists in Seoul over fourteen months has surfaced both the promise of this model, meaningful collective bargaining power, and its operational costs, including legal-structuring expenses and the ongoing labour of hybrid, participatory decision-making.

Extended collective licensing, adapted from existing music-industry rights-management infrastructure, offers another route: enabling AI developers to license cultural training data at scale through a collective body, with built-in audit rights and revenue-sharing. Provenance and consent infrastructure, technical standards that allow training data to carry traceable metadata about origin and licensing terms, would make Training Data Justice more technically enforceable, though current standards remain unevenly adopted and were not originally designed with cultural-community consent in mind.

At the policy level, treating training data explicitly as public infrastructure, rather than as a private commercial input, is a reframing several Asia-Pacific governments are beginning to explore.

Open questions remain substantial. How should consent be operationalised for cultural material whose original creators are deceased, dispersed, or constituted as a community rather than identifiable individuals? Can attribution and benefit-sharing mechanisms be made technically workable once data has already been absorbed into existing trained models? And can Training Data Justice be implemented through voluntary, ethics-led frameworks, or does

meaningful cultural sustainability in the AI era require binding legal obligation, and at what jurisdictional level can that obligation realistically be enforced against transnational AI development?

Mechanisms at a glance

Mechanism	What it does
Cultural Data Trusts	Community-governed legal structures for collective licensing, consent management, and benefit-sharing — piloted in Seoul with 50 founding artist members over 14 months.
Extended Collective Licensing (ECL)	Music-industry-derived model enabling AI developers to license training data at scale through a collective body, with audit rights and revenue-sharing.
Provenance / Consent Metadata	Technical standards (e.g. C2PA) allowing training data to carry traceable origin and licensing information.
Training Data as Public Infrastructure	Policy reframing positioning cultural training data as a public-interest asset requiring governance, not a private commercial input.

References

[1] UNESCO, Recommendation on the Ethics of Artificial Intelligence, UNESCO Publishing, 2021. https://unesdoc.unesco.org/ark:/48223/pf0000381137

[2] 'Disney, Universal sue Midjourney over AI copyright' The Washington Post, 11 June 2025. https://www.washingtonpost.com/technology/2025/06/11/disney-universal-sue-midjourney-ai-copyright/ accessed 9.09.2025

[3] Noh, M. J. 'Training Data Justice, Cultural Sovereignty, and Decolonial AI Governance: A Global South Perspective' Islamic Studies in the Global South (ISGS), 1(2), 2026. https://journal.surplusrc.id/index.php/isgs/article/view/16

[4] 'Governance of Generative AI in Creative Work: Consent, Credit, Compensation, and Beyond' https://arxiv.org/pdf/2501.11457

[5] 'Copying Style, Extracting Value: Illustrators' Perception of AI Style Transfer and its Impact on Creative Labor' https://arxiv.org/abs/2409.17410

[6] Society of Authors, survey on translators and illustrators losing work to AI, 2024. https://societyofauthors.org/2024/04/11/soa-survey-reveals-a-third-of-translators-and-quarter-of-illustrators-losing-work-to-ai/ accessed 9.09.2025

[7] Foka, A. 'She Works, He Works: A Curious Exploration of Gender Bias in AI-Generated Imagery' https://arxiv.org/abs/2407.18524

[8] Joint Statement on Generative Artificial Intelligence and the EU AI Act, European Writers' Council, 2024. https://europeanwriterscouncil.eu/240425_cwos_jointstatement_ai-act/

[9] Ethical impact assessment: a tool of the Recommendation on the Ethics of Artificial Intelligence, UNESCO, 2023. https://unesdoc.unesco.org/ark:/48223/pf0000386276

[10] AI Impact Alliance / UNESCO Civil Society and Academic Network on AI Ethics & Policy, Repository on AI, Intellectual Property, and Culture (workshop contribution), 2026. https://www.allianceimpact.org/

[11] Noh, M. J. 'Beyond Copyright: Why Asia Pacific Governments Must Govern AI Training Data as Public Infrastructure' GovInsider Asia, March 2026. https://govinsider.asia/intl-en/article/beyond-copyright-why-asia-pacific-governments-must-govern-ai-training-data-as-public-infrastructure?utm_content=bufferd1960&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer

[12] Noh, M. J. (2026). Curating Intelligence: The Playbook for Art, Governance, and the New Global Economy. ARTLAKE Inc.

e Book: https://a.co/d/09ZEj35T

Paper Book: https://a.co/d/0gTal4p8

AUTHOR

Mika (Jaeyun) Noh is an AI governance and cultural policy strategist specializing in the intersection of artificial intelligence, cultural sustainability, digital sovereignty, and the creative economy. Drawing on experience in the National Assembly of Korea, the Ministry of Culture, Sports and Tourism, and international policy initiatives, she develops governance frameworks that align technological innovation with cultural rights and democratic values. She is the author of Curating Intelligence: The Playbook for Art, Governance, and the New Global Economy (2026) and has published widely on AI governance, platform governance, and cultural policy. Her current research introduces concepts including Training Data Justice, Cultural Data Trusts, and Algorithmic Cultural Mapping to advance more inclusive, participatory, and human-centered AI governance.

Beyond data: Why culture and human judgement matter for institutions in the age of AI

Elena Raevskikh
Research & Analysis Unit Head, Department of Culture and Tourism Abu Dhabi

Giovanna Di Mauro
Senior Researcher, Department of Culture and Tourism

- AI is transforming the production and accessibility of information, shifting the strategic challenge from knowledge creation to the exercise of judgement.
- Culture can provide the interpretative foundations through which we assign meaning, negotiate priorities and translate decisions into legitimate action.
- In the era of AI, culture will play an increasingly important role as a strategic asset by strengthening the capacity of societies to govern complexity.

In his epic novel *Crime and Punishment*, Fyodor Dostoyevsky places moral responsibility at the centre of human freedom, suggesting that knowledge alone is insufficient without ethical accountability for how meaning is interpreted and acted upon.

As governments move towards anticipatory and artificial intelligence (AI)-enabled models, the boundary between information and human judgement

becomes increasingly important. In a world saturated with data, the defining question is no longer what societies know, but how they determine what matters.

This is ultimately a cultural question. Culture provides the shared frameworks through which information acquires significance, priorities are negotiated and collective action becomes possible.

AI can process information at scales impossible for human beings and reveal relationships that would otherwise remain unexplored. A digital twin may reveal that a historic neighbourhood is experiencing demographic change, just as an algorithm may identify a school district facing educational inequities.

Yet neither system can determine whether preserving local identity should take precedence over redevelopment, or whether resources should be directed towards equity, excellence or efficiency. Information can reveal conditions; it cannot determine their significance.

Societal frameworks for interpreting reality

As French sociologist and anthropologist Marcel Mauss observed, societies inherit not only knowledge but also shared frameworks for interpreting reality. Facts do not speak for themselves: their meaning emerges through collective experience, institutional practice and cultural context. This is particularly relevant when decisions concern cultural heritage, education, health or social welfare.

A predictive AI model may identify which heritage sites are most vulnerable to deterioration, but it cannot determine why one site should be prioritized over another, especially when communities attribute different forms of historical, symbolic or cultural value to each. Evidence remains essential, but it cannot determine what should be preserved, prioritized or transformed. Such decisions depend on interpretation, responsibility and public legitimacy.

While digital systems are highly effective at preserving information, they are far less effective at replicating the human capacity to interpret information, assign meaning and exercise judgement.

As governments move towards more anticipatory and AI-enabled models of governance, the distinction between information and meaning becomes increasingly important. Across the world, public institutions are redesigning services around people's lives rather than administrative structures.

Abu Dhabi's anticipatory-government model, New Zealand's well-being framework and the growing adoption of anticipatory governance across Organisation for Economic Co-operation and Development (OECD) countries illustrate some aspects of this evolution.

Yet they also reveal an important boundary: the more routine decisions become automated, the more visible becomes the category of decisions that cannot be automated. Questions concerning life events, community life or cultural continuity cannot be resolved solely through optimization. They require judgement in determining where automation ends and individual responsibility begins.

The strategic value of human judgement

Artificial intelligence can expand analytical capabilities, but innovation ultimately depends on human judgement: the capacity to situate information within lived reality, relate facts to values, understand consequences and assume responsibility for action.

The same evolution is taking place in the way institutions approach knowledge. For many years, organizations focused on knowledge management: collecting information, documenting expertise and improving access to data. Increasingly, the challenge concerns knowledge governance: ensuring that information, expertise and experience can be translated into legitimate action.

This distinction matters because not all knowledge can be codified. As the Hungarian-British polymath Michael Polanyi observed, we know more than we can tell. Professional expertise often depends on experience, contextual understanding and practical judgement that cannot be fully reduced to procedures or algorithms.

> *Not all knowledge can be codified. As Michael Polanyi observed, we know more than we can tell"*

A conservation specialist assessing a historic structure, a teacher responding to the needs of a particular classroom or a physician interpreting a complex diagnosis all draw upon forms of tacit knowledge that emerge through practice rather than formal instruction. Some forms of expertise survive not because they are documented, but because they are transmitted through communities of practice and institutional cultures.

Consequently, the challenge for AI-era institutions is not simply to store more knowledge, but to preserve the conditions through which knowledge supports meaningful judgements.

Culture as infrastructure for interpretation

Culture is often discussed through the lens of heritage, participation, tourism or the creative economy. Yet its contribution extends beyond these domains. Just like physical infrastructure supports mobility and digital infrastructure facilitates connectivity, culture enables interpretation.

It provides the shared references and values through which societies make sense of change. The capacity to judge is rarely created at the moment a decision is made. Instead, it is accumulated over time through shared experience, collective memory and cultural practice.

For this reason, culture should be understood not only as a sector, but also as an enabling system for governance. It strengthens the interpretative capacity upon which public institutions depend when navigating uncertainty, complexity and competing priorities.

One consequence of this perspective is that cultural measurement must evolve. For decades, cultural indicators focused primarily on participation, attendance, employment and economic contribution.

As highlighted by Pope Leo XIV in the *Magnifica Humanitas*, these metrics almost systematically neglect aspects essential to the overall well-being of people and the environment. Thus, the challenge is increasingly to understand how culture contributes to resilience, trust, social cohesion, adaptability and institutional learning. These dimensions are harder to quantify, yet they become valuable in times of technological and social transformation.

Experience from Abu Dhabi illustrates this transition. Building cultural indicators required moving beyond standardised measurement frameworks and engaging with locally relevant forms of value. The objective was not simply to measure cultural activity, but to understand culture's contribution to broader development outcomes and institutional capacity.

Culture as a strategic asset in the age of AI

The transition now under way is often described as a shift towards AI-native institutions. Yet the deeper transformation concerns human judgement itself. As artificial intelligence becomes more pervasive, the less visible cultural capacities that support interpretation, responsibility and legitimacy become more important.

Cultural and educational institutions occupy a particularly important place within this agenda. Their contribution extends beyond the transmission of knowledge or the preservation of heritage.

Museums, libraries, archives, schools and universities preserve memory, contextualize information and expose individuals to multiple perspectives and competing narratives. In doing so, they cultivate capacities that become increasingly valuable in an age of AI: the ability to exercise judgement, navigate complexity and understand the broader consequences of decisions.

In this context, culture is not simply a beneficiary of innovation: it forms part of the enabling environment through which institutions learn, adapt and maintain legitimacy.

From this perspective, culture becomes a strategic asset because it strengthens the capacity of societies to govern complexity. As AI expands the availability of information, the critical challenge lies in transforming information into meaning and meaning into judgement. Yet judgement itself is not the final objective. Public institutions must also secure legitimacy: the capacity to justify decisions, command trust and maintain collective confidence.

Culture provides the interpretative foundations through which this legitimacy is constructed. In this sense, the debate extends beyond AI governance itself. The more capable technological systems become, the more strategic culture becomes as the framework through which societies determine what matters, exercise judgement and translate knowledge into legitimate action.

This insight echoes one of Dostoyevsky's enduring themes: knowledge and reason alone are insufficient without moral responsibility. As institutions enter an era increasingly shaped by artificial intelligence, the challenge is not only to build smarter systems, but also to strengthen the cultural foundations that enable judgement, legitimacy and responsible action.

Article originally published on the World Economic Forum:
https://www.weforum.org/stories/2026/06/beyond-data-culture-human-judgement-institutions-ai/

AUTHORS

Elena Raevskikh is a Research & Analysis Unit Head, at the Department of Culture and Tourism Abu Dhabi. Elena Raevskikh holds a Ph.D. in Sociology from EHESS and a degree in Public International Law from Moscow State University. Beyond being Head of the Research and Analysis Unit of the Department of Culture and Tourism of Abu Dhabi, she leads and co-develops CultureSTATS-AD, the first initiative of its kind in the MENA region dedicated to creating tailored qualitative and quantitative measurements for Abu Dhabi's culture sector. Since 2020, her team has produced more than 20 research reports, including the landmark Abu Dhabi Cultural Activities Baseline Report (2021), several in-depth studies on creative ecosystems, and economic analyses of the emirate's culture sector, with findings published in leading international journals such as Quality & Quantity and Nature. Her work has also shaped the biennial Abu Dhabi Culture Population Survey, the region's first Register of Cultural Organizations and Professionals, and new heritage and cultural destination indicators. At the Department of Culture and Tourism – Abu Dhabi, she collaborates with UNESCO, OECD, IFACCA, ENCATC, WCCF, and the World Economic Forum, linking local practice with global dialogues on culture, sustainability, and innovation.

Giovanna Di Mauro is a Senior Researcher, at the Department of Culture and Tourism. She has taught at Zayed University (College of Interdisciplinary Studies), King's College London (School of Security Studies), Collegium Civitas in Warsaw (Department of Peace and Conflict Studies), and the University of St Andrews (School of International Relations). Giovanna holds a PhD in International Relations from the University of St Andrews (UK), a Master's degree in Expressive Arts, Peacebuilding, and Conflict Transformation from the European Graduate School (Switzerland), and a Bachelor's degree from the University of Naples 'L' Orientale' (Italy).

Cyber Humanities for Heritage Security

Emanuele Bellini
Associate Professor in Information Processing Systems

By bridging the gap between humanities and technologies, cyber humanities aims to develop innovative skills and competencies to protect digital cultural assets from cyber threats.

In recent years, the foundational certainties that once underpinned our sense of security have eroded in the face of escalating geopolitical tensions and digital vulnerabilities. The war in Ukraine stands as a watershed moment, reshaping global perspectives on the protection and preservation of digital cultural heritage. As the world becomes increasingly unstable and hostile, cultural heritage—long targeted for physical destruction, as seen with the Buddhas of Bamiyan, the devastation of Palmyra, and the ongoing looting of artifacts and theft of works of art—is now equally at risk in the digital realm. Vulnerability of the digital surface, enabled through digital transformation, to cyberattacks combined with the low cost and high impact of malware, ransomware, and so forth, is pressuring the cultural heritage domain in a way that has never been seen before. This growing threat is underscored by a wave of cyberattacks against major cultural institutions, such as the Metropolitan Opera (2022), the British Library (2023), the Berlin Natural History Museum (2023), the Seattle Public Library (2024), the Louvre (2024) and 40 other museums, and the Internet Archive (2024). As Internet Archive founder Brewster Kahle noted in response to these attacks: "What is new is this attack has been sustained, impactful, targeted, adaptive, and importantly, mean."[11] In this context, new skills and expertise are essential to protecting digital cultural heritage in an increasingly hostile digital landscape and to supporting its transformation, as the rise in cyber threats becomes more severe.

The Fragility of Digital Cultural Heritage: Lack of Cyber Resilience

These escalating cyber threats reveal an alarming reality: We are entering a more hostile world, and most societal sectors—especially cultural heritage—are ill-prepared to confront this new landscape. What is lacking is the culture of cyber security and resilience that is stressed in domains considered critical to the functioning of society, such as energy or transport. Using Hollnagel's resilience framework,[12] which defines resilience through four key capabilities, we can pinpoint critical failures that expose the fragility of the cultural domain.

- *Failure of knowing what to expect (Anticipate)*: The cultural heritage domain is failing to identify potential sources of disruption or pressures that may compromise operations. This results from a false sense of security,[20] where the openness and perceived stability and neutrality of existing cultural information systems covers their actual fragility. This widely held perception led organizations to focus on more traditional issues, such as long-term digital preservation, curation, and accessibility of digital objects. This is also evident in the recent UNESCO PERSIST project, launched in 2021, where the considered risks are limited to format obsolescence, hardware failure, and financial issues, while cyber threats seem to be neglected.

- *Failure in knowing what to do (Respond)*: When faced with disruptions, the domain struggles to adapt. This is caused by a lack of resources (Kahle thanks some commercial companies that have offered assistance to the Internet Archive that would generally be prohibitively expensive for cultural heritage organizations), insufficient competencies available in cultural institutions, and the slow pace of adaptation to digital transformation. Moreover, the on-premises/siloed approach of content management combined with the widespread presence of legacy ICT systems, is a very typical condition in heritage institutions. This creates a vulnerable single point of failure that increases the risk of cyber incidents.

- *Failure in knowing what to look for (Monitor)*: The growing complexity of digital cultural heritage amplifies the risk of cascade effects, where the consequences of attacks reverberate across scales of time and space. These effects of attacks can be categorized into short-, mid-, and long-term impacts. *Short-term effects* involve immediate service disruption, often

caused by sabotage, vandalism, or ransomware. For instance, restricted access to digitized manuscripts can hinder research and education, with global repercussions for cultural institutions, leading to significant recovery costs. *Mid-term effects* stem from cyber-cognitive operations aimed at damaging institutional reputation and trust in digital content. Techniques such as man-in-the-middle attacks, quantum attacks on digital signatures, and hash collisions raise doubts about the authenticity of preserved materials. *Long-term effects* result from advanced persistent threats designed to alter cultural identity. By poisoning archives with fake or manipulated cultural artifacts—such as deepfake images, forged handwriting, and text alterations—attackers can distort historical narratives, making detection increasingly difficult.

- *Failure in knowing what has happened (Learning)*: Learning requires a rigorous examination of both successes and failures, enabling the cultural heritage sector to confront the factual and draw actionable insights for rapid actions. According to the BBC, in Ukraine 139 religious sites, 214 buildings of historical or artistic interest, 31 museums, 32 monuments, 15 libraries, and one archive have all been attacked. Natural disasters, such as the flooding in Florence, Italy in November 1966, and man-made incidents (for example, the fire at the Notre Dame Cathedral in Paris) further exemplify the vulnerability of cultural heritage. Digitizing analog artifacts is a crucial strategy to prevent irreversible cultural loss. However, the cultural sector is too slow in adapting processes to countermeasures. The brightest example is represented by the MD5. It had to be discontinued in 2008 just after the publication of the proof of collision shown at the 25th Chaos Communication Congress,[23] but it is still used in several cultural information systems.

Toward Cyber Humanities: A Transdisciplinary Evolution

Since its emergence in the 1960s, digital humanities (DH) has evolved into a highly multidisciplinary field aimed at using digital tools to enhance humanities disciplines, but the technological and humanistic domains have often followed parallel trajectories, converging only sporadically and frequently struggling to establish meaningful dialogue. In fact, DH has primarily been led by humanists, who often adapt and customize existing technologies that often were originally

developed within hard science for other purposes. Notable examples include the Open Archival Information System (OAIS) (ISO 14721:2012[13]) elaborated within the space domain or the IETF-standardized Handle System,[14] designed by Bob Kahn to ensure the persistent identification of online digital objects. These technologies have been widely adopted in digital archives and libraries due to their relevance for digital preservation and content citation (for example, DOI[22]). The digital turn has ushered in a paradigm shift, vastly expanding the possibilities offered by ICT, but new challenges are arising from this shift that require more than just multidisciplinary collaboration; they demand a new, trans-disciplinary approach. Cyber-humanities, as a new discipline, aims at actively engaging the hard sciences in solving humanities-related challenges, fostering technological innovation, and developing new methodologies for safely integrating the humanities into cyberspace. The concept of transdisciplinarity, first introduced by Jean Piaget and later expanded by Basarab Nicolescu, embraces a holistic, multidimensional approach to problem-solving. Cyber humanities transcends conventional disciplinary boundaries, fostering the integration of knowledge rather than merely juxtaposing different fields. Thus, unlike the utopian "epistemological polyglotism" critiqued by Blanchard-Laville, cyber humanities embodies the vision of UNESCO that defines transdisciplinarity as an "intellectual space," where interconnected issues are explored, alternative perspectives are reconsidered, and relationships between disciplines are revealed.[25]

Cultural cyber critical ecosystem

The object of cyber humanities studies is the digital heritage recognized as a cultural cyber critical ecosystem (C3E) (see Figure 1). The ecosystem metaphor underscores the interdependence of various elements within this informational environment—what Floridi refers to as "inforgs" inhabiting the "infosphere."[10] Thus, C3E is composed by complementary entities that are not only interconnected, but inter-reliant and work together to achieve a common value proposition or mission. C3E should be considered critical since it "is crucial for the maintenance of vital societal functions" (Council Directive 2022/2557/EC on Resilience of Critical Entities). In fact, it is imperative to treat the (digital) culture heritage as a critical infrastructure because of its role in shaping the society's identity and cohesion. According to Vespignani,[27] critical infrastructures are complex systems for which it is generally impossible to abstract the global behavior from the analysis of

single components. This reflects C3E characteristics since it is intrinsically under-specified, exhibits non-linear dynamics in case of perturbation, and interacts with the environment. Therefore, analyzing the behaviors, interactions, interdependencies, and performance of such a complex system is part of the scope of cyber humanities. Like other ecosystems, C3E has a purpose (mission) and it is composed by: assets, agents, and functions through which assets are manipulated by the agents; and infrastructures to enable and support functions and interactions. It should also exhibit specific properties, such as resilience, trust, and sustainability, to maintain equilibrium and continue serving the mission.

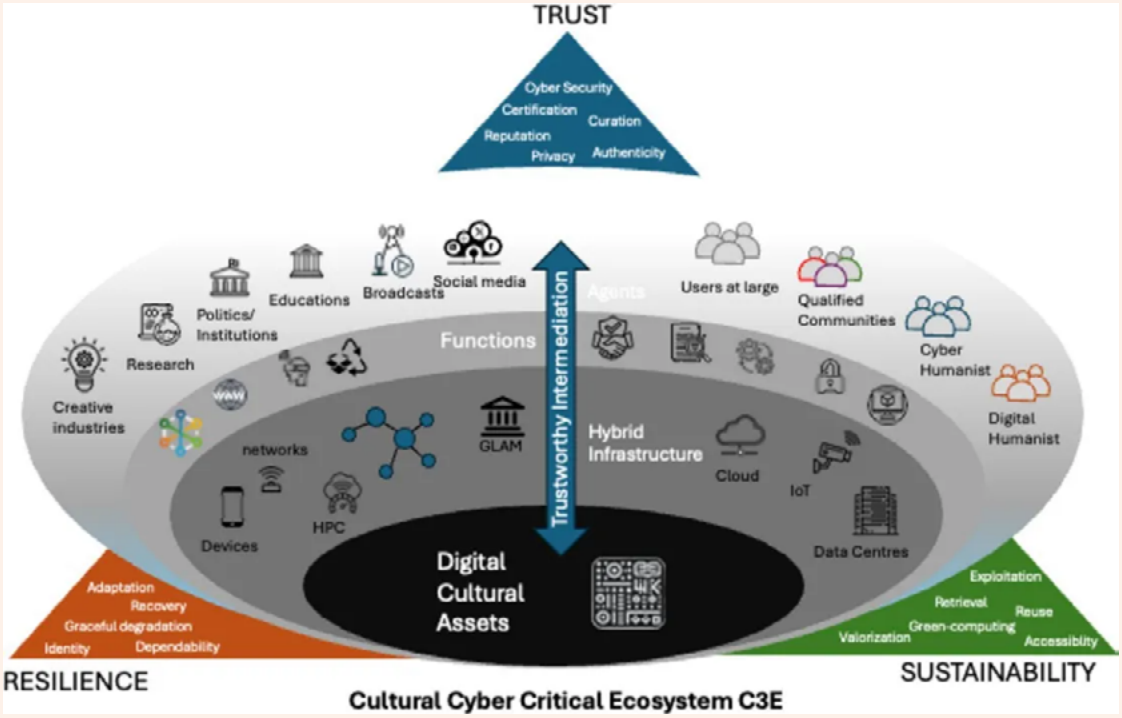


Figure 1. Cultural Cyber Critical Ecosystem—C3E.

Mission. The mission of C3E is to support trustworthy digital heritagization, preservation, protection, accessibility, and understandability over the course of a digital cultural asset's time to secure its "interoperability with the future."[6,22] C3E's mission is inspired by Moore's theory of digital preservation, whereby

effective preservation environments "validate communication from the past … while communicating with the future,"[18] and by the digital heritagization where born-digital and digitized heritage converge.[9,19] In particular, digital heritagization can be considered a process shaped by human organization and hybrid agents[1] that blends social and technical mediations. This multi-layered system highlights the diversity of actors, motivations, and socio-technical devices involved in heritagization.[19] The C3E should ensure that such a process is conducted in a trustworthy environment.

Agents. Agents are whomever interacts with digital cultural assets (DCAs), including communities (e.g., galleries, libraries, archives, and museums, cultural operators, users at large), organizations (research, educational, creative, mass media, social media), and software agents.

Assets. C3E is DCA-centered. The DCA is the output of a digital heritagization, and includes anything digital that has a cultural significance. It includes a diverse array of information objects, such as resources, annotations, metadata, and paradata among others. DCA significance is multivalent and community-related[9] but needs to be quantified to support risk-informed decision making on it (e.g., what resources are needed to preserve and protect a DCA? How can investments be prioritized?). We can identify three main macro-criteria for the significance quantification:

- Production costs are related to the costs of digitization or production (if born-digital) of the digital cultural artifacts. They are influenced by the technologies used, the quality of the digital surrogate, expertise of the staff employed, time consumed.

- Functional value describes how a DCA can be used or reused in the production process; it holds value as property. Its definition is contingent and market driven. We can adopt a value-driven approach where, according to the Vale Network Analysis, the value of DCA is co-created through the continuous interactions among agents and within the DCA.

- Cultural value is assigned by experts on the base of historical and cultural considerations. This is related to the selection that cultural operators perform every day on cultural contents.

Cyber humanities will be devoted to investigating such criteria and their implications in decision making, optimization, value exploitation, and protection through the design and adoption of dedicated technologies.

Functions. C3E functions include all technical operations that can be performed on a DCA along its lifecycle. They can be categorized as functions for digitization, curation, storage, preservation, protection, retrieval, analysis, access, reuse, and so forth. Each function is based on technologies that require specific competencies at both humanistic and technological levels on their design and use. Examples of such competencies include remote sensing/IoT for digitization and monitoring, ML/AI for content recognition, LLM+RAG for information retrieval, cybersecurity for data protection, and extended reality for valorization and user engagement.

Hybrid infrastructure systems. Hybrid infrastructure (HI) systems are the backbone of C3E and should be recognized as dynamic multilayered networked systems. HI systems are hybrid because they include interdependent physical, cyber, and social layers. The *physical layer* can include such things as library, museum, archive, and gallery buildings, datacenters, communication infrastructures, devices, sensors; the *cyber layer* includes applications (e.g., digital library systems), cloud services, tools, protocols, process, data, and business logic; and the *social layer* is represented by operators, curators, practitioners, researchers, cultural industries, and end users, as well as by policies and norms. HI embodies the convergence of the cyber-physical world, immersing humans in a continuous exchange of information between the physical and cyber realms.[7] In the evolving Internet of Everything (IoE) and Connected Community paradigms,[4] people remain constantly connected, forming dynamic, thematic communities. These communities require seamless access to trustworthy DCAs anytime, anywhere to enhance their understanding and interpretation of the world.

Properties. What are the significant characteristics of C3E that are necessary to carry out the mission of the ecosystem? We identified three essential properties the C3E should exhibit to accomplish its missions and secure its existence: *trust, resilience,* and *sustainability*. These properties must be maintained simultaneously, as they are interdependent and cannot substitute or compensate for one another.

Trust: Since it is an open ecosystem, C3E operates in a partially trusted environment, where cultural institutions help ensure the trustworthiness of DCAs, while access and reuse remain largely open, minimizing certification requirements. Unlike sectors such as Bitcoin, which rely on computational consensus for trust, C3E depends on trustworthy intermediation with institutions that play a key role in ensuring trust by authenticating DCA, preserving their significant properties (content, context, appearance, structure, behaviour) in a long-term, and facilitating reliable interactions with them. The bricks of trust model[3]—comprising elements such as technology, organization, financial, commitment, and mandate—provides a framework for securing trust, which, as Luhmann noted,[17] reduces complexity and mitigates risk. Trust can be reinforced through certifications such as ISO 14721:2012, ISO 16363:2013, CoreTrustSeal and DIN 31644, aligning with critical infrastructure standards. Technologically, securing DCA involves solutions such as fully homomorphic encryption, secure multi-party computation, confidential computing, distributed ledger technology, and X.509 certificates. However, these advanced tools remain largely inaccessible to cultural heritage institutions due to high cost and skill requirements. Cyber humanities aims to address this issue by creating a new army of experts, the *cyber humanist*, able to manage such technologies in humanities domain and implement the first line of defense in the cultural heritage organizations.

Resilience: Resilience is a multifaceted concept, and its application to C3E presents unique challenges. Various definitions exist[2] and emphasize different aspects, such as the persistence of system dependability,[15] identity preservation,[8] adaptability,[12] and graceful extensibility[28] when facing "unknown unknowns."[21] A comprehensive approach must integrate these perspectives. We adopt a holistic view, drawing on Aristotle's concepts of potency and action to combine the concept of potential for

resilience (design time) with the concept of resilience as an emergent property related to the behavior performance of a system (runtime).[5] At design time, resilience potential in C3E can be assessed through ecosystem characteristics—redundancy, diversity, modularity, connectivity, adaptability, and evolvability—as well as available resources such as human capital, finances, technology, and organization. These elements contribute to four key capacities: anticipation, response, monitoring, and learning. At runtime, resilience is measured through system performance, focusing on disruption absorption (the extent of output loss) and recovery time. For C3E, this output corresponds to its ability to support the DCA lifecycle.

- *Sustainability*: Ensuring the long-term sustainability of C3E is essential to fulfilling its mission and maintaining the value of DCA. Self-sustainability depends on protecting or enhancing this value across technical, environmental, organizational, cultural, and economic dimensions. For example, sustainability can be addressed technologically through energy-efficient computing to reduce costs and environmental impact or implementing scalable architecture, while at the organizational level, skilled human capital is crucial. Sustainability also plays a key role in the resilience vs. efficiency trade-off, which is particularly challenging for the heritage sector. While resilience investments may initially reduce short-term efficiency due to cost-functionality constraints[16] (risking an initial assessment of unsustainability), in the long run, non-resilient systems incur higher overall costs,[26] falling into an unsustainable area. To assess whether sustaining C3E is viable, cyber humanities should incorporate methodologies such as multi-criteria decision analysis and cost-benefit analysis to ensure informed decision making in balancing resilience and efficiency.

Conclusion

Cyber humanities is an emerging field still defining its scientific, practical, and skill-based boundaries. However, the cultural-heritage sector urgently needs specialized expertise to drive its digital transformation—expertise not yet fully addressed by current education systems. To bridge this gap, transdisciplinary pathways must integrate foundational and emerging technologies with the

specific needs of humanities and culture. Cyber humanities envisions cultural heritage as a cultural cyber critical ecosystem with significant societal impact, enabling better resource mobilization for its protection, resilience, and continuity. As a transdisciplinary domain, cyber humanities redefines the intersection of humanities and technology, fostering research, innovation, and the adoption of sustainable digital practices. It aims to stimulate research and innovation in the scientific and technological sectors while fostering the adoption of sustainable and cutting-edge technologies throughout the digital resource lifecycle. Notable examples are the Saving Ukrainian Cultural Heritage Online (SUCHO) Initiative, 24 which mobilized volunteers to transfer 50TB of Ukrainian cultural heritage data to Stanford servers, safeguarding invaluable DCA from destruction during conflict; and the Notre Dame Cathedral restoration project that leveraged advanced technologies for the reconstruction. Beyond its technological implications, cyber humanities serves as a catalyst for interdisciplinarity; it promotes cross-fertilization between technical and humanistic disciplines, shaping the future of heritage research, preservation, and engagement.

A new discipline is born.

References

1. Abbate, J. L'histoire de l'Internet au prisme des STS. *Le Temps des médias* 18, 1 (2012), 170–180; doi:10.3917/tdm.018.0170
2. Alhidaifi, S.M., Asghar, M.R., and Ansari, I.S. A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM Comput. Surv.* 56, 8, Article 196 (Apr. 2024), 48; doi:10.1145/3649218
3. Bellini, E. et al. NBN:IT The Italian trusted persistent identifier infrastructure. *Intern. J. of Knowledge and Learning* 9, 4 (2014), 347–363; doi:10.1504/IJKL.2014.069536
4. Bellini, E., Ceravolo, P., and Nesi, P. Quantify resilience enhancement of UTS through exploiting connected community and Internet of Everything emerging technologies. *ACM Trans. Internet Technol.* 18, 1, Article 7 (Oct. 2017), 34; doi:10.1145/3137572
5. Bellini, E. and Marrone, S. Towards a novel conceptualization of cyber resilience. In *Proceedings of the 2020 IEEE World Congress on Services (SERVICES)* (2020), 189–196; doi:10.1109/SERVICES48979.2020.00048

6. Chassanoff, A. and Altman, M. Curation as 'interoperability with the future': Preserving scholarly research software in academic libraries. *J. of the Association for Information Science and Technology* 71, 3 (2020), 325–337; doi:10.1002/asi.24244, https://tinyurl.com/2d8r6skh

7. Conti, M. et al. Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence. *Pervasive and Mobile Computing* 8, 1 (2012), 2–21; doi:10.1016/j.pmcj.2011.10.001

8. Cumming, G.S. and Collier, J. Change and identity in complex systems. *Ecology and Society* 10, 1 (2005); https://tinyurl.com/27jwuuwy

9. Davallon, J. *Constructing cultural and natural heritage.* Documenta Universitaria, Chapter 3: The Game of Heritagization (2010), 25–48; https://tinyurl.com/28wslwxu

10. Floridi, L. Digital's cleaving power and its consequences. *Philosophy and Technology* 30 (May 2017), 123–129; doi:10.1007/s13347-017-0259-1

11. Freeland, C. Internet Archive and the Wayback Machine under DDoS cyber-attack. *Internet Archive* (2024); https://tinyurl.com/267x7jvh

12. Hollnagel, E. and Woods, D. Epilogue: *Resilience Engineering Concepts and Precepts*. Ashgate (2006), 347–358.

13. ISO 14721:2012. Space data and information transfer systems—Open archival information systems (OAIS)—Reference model (2012); https://tinyurl.com/2xzyhptt

14. Kahn, R. and Wilensky, R. A framework for distributed digital object services. *Intern. J. on Digital Libraries* (2006), 115–123; doi:10.1007/s00799-005-0128-x

15. Laprie, J. From dependability to resilience. In *Proceedings of the IEEE Conf. Dependable Systems and Networks* (2008).

16. Linkov, I. et al. Cyber efficiency and cyber resilience. *Commun. ACM* 66, 4 (March 2023), 33–37; doi:10.1145/3549073

17. Luhmann, N. Trust: A mechanism for the reduction of social complexity. *In Trust and Power*, N.Luhmann (Ed.). Wiley (1979), 4–103.

18. Moore, R. Towards a theory of digital preservation. *Intern. J. of Digital Curation* 1 (Jan 2008); doi:10.2218/ijdc.v3i1.42

19. Musiani, F. and Schafer, V. Digital heritage and heritagization. *RESET* 6 (2016), 170–180; doi:10.3917/tdm.018.0170

20. Nguyen, C.D. Digital cultural heritage in the crossfire of conflict: cyber threats and cybersecurity perspectives. *Insights*: The UKSG J. (May 2024); doi:10.1629/uksg.647

21. Park, J. et al. Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis* 3, 3 (2013), 356–367; doi:10.1111/j.1539-6924.2012.01885.x, arXiv:https://tinyurl.com/262b8vhc

22. Paskin, N. Digital object identifiers for scientific data. *Data Science J.* (Jan. 2006); doi:10.2481/dsj.4.12

23. Sotirov, A. et al. MD5 considered harmful today: Creating a rogue CA certificate. (2008); https://tinyurl.com/2awnwx8e

24. SUCHO Project; https://www.sucho.org/

25. UNESCO. Transdisciplinarity: Stimulating synergies, integrating knowledge. In *Proceedings of the Intern. Symp. on Transdisciplinarity* (1998); https://unesdoc.unesco.org/ark:/48223/pf0000114694

26. Vardi, M.Y. Efficiency vs. resilience: What COVID-19 teaches computing. *Commun. ACM* 63, 5 (Apr.2020), 9; doi:10.1145/3388890

27. Vespignani, A. The fragility of interdependency. *Nature 464* (2010), 984–985; doi:10.1038/464984a

28. Woods, D.D. The theory of graceful extensibility: Basic rules that govern adaptive systems. *Environment Systems and Decisions* 38, 4 (2018), 433–457; doi:10.1007/s10669-018-9708-3

This article was first published on Communications of the ACM
Cyber Humanities for Heritage Security

AUTHOR

Emanuele Bellini Associate Professor in Information Processing Systems and Director of the 2nd Level Master in Cyber Humanities for Heritage Security at the Department of Humanities Studies at University of Roma Tre, Italy. Chair of the IEEE SMC TC on Cyber Humanities and co-chair of IEEE SMC TC on Homeland Security, Italy.

ENCATC RESOURCES

Designed for your cultural management and policy needs

Your trusted resources anytime, anywhere

All of our ENCATC resources are available in one place and in easy to use e-formats.
Learn more and visit us on the web at: https://www.encatc.org/en/resources/

NEVER MISS A BEAT!

TWICE-YEARLY

ENCATC Magazine

An essential weekly must-read for the latest news and happenings in cultural management and policy. Always benefit from a free publication, a rich offer of training and networking events, and opportunities to advance policy and projects.

/encatcSCHOLAR

This is a unique tool for education and lifelong learning on arts and cultural management and policy. With the teaching needs of educators and trainers in mind, we publish unique content, exclusive interviews, case studies, conference reports and more from around the globe and across sectors useful for the classroom and lifelong learning.

YEARLY

European Journal of Cultural Management and Policy

Be part of the stimulating debate on hot research topics in our field happening among scholars, educators, policy makers and cultural managers. Benefit from the Journal's scientific rigor to bring you a multidisciplinary perspective bridging theory and practice.

ENCATC Book Series on Cultural Management and Cultural Policy Education

Designed to promote the work of young promising researchers, this series is a must for your university library or collection on the topic of cultural management and policy.

Congress Proceedings

Nowhere else will you find a collection of articles on cultural management and policy and with such expansive geographic coverage. Stay on top of the newest research being conducted each year in the field.

WEEKLY

ENCATC Flash

An essential weekly must-read for the latest news and happenings in cultural management and policy. Always benefit from a free publication, a rich offer of training and networking events, and opportunities to advance policy and projects.

MONTHLY

ENCATC Newsletter

Feeling too much is happening too fast? Our members can be at ease as we do the work to find and compile key policy developments from the EU and other world regions, calls, publications, events, conferences and more. Gain access to what you and your institution need to stay on top of progress and opportunities in our field.

THREE TIMES-YEARLY

ENCATC Tracker

The Cultural Policy Tracker is a quarterly publication contributing to the development of evidence-based cultural policies promoting and advocating for innovative policies and practices in the cultural and creative sectors. It is widely disseminated to policymakers.

JOIN US!

Together we have the power to make the education and cultural sectors stronger and more sustainable!

By joining ENCATC you will have the opportunity to:

1. Influence the international, European, national and regional culture and education policy by engaging in our policy statements and publications
2. Connect with a global network of HEI and cultural institutions to find project partners and collaborators
3. Enhance your organisation's visibility outside your own country by joining our labelling programme and publishing in our newsletters, flashes, and magazine
4. Have exclusive access to the ENCATC Breakfast Webinars and Members Talks
5. Receive a 30% discount to attend the ENCATC Annual Congress, Education and Research Session, Academy, and International Study Tour
6. Be eligible for a mobility grant to attend our events (Thomassen Fund)
7. Access the Members Area with teaching materials, resources, and the ENCATC online international bibliography including at date more than 2,000 references
8. Receive one-year subscription to our monthly newsletter for members and our monthly PRAXIS newsletter for your students and young professionals
9. Receive weekly ENCATC Flash update in the field of cultural policy and management
10. Link education with placement opportunities thanks to the ENCATC Marie Claire Ricome Programme now offering virtual traineeships for 2020

FULL MEMBER

Higher education institutions and training centres providing recognised education and training programmes on cultural management and policy

500 EUR | JOIN!

ASSOCIATE MEMBER

Organisations, institutions and networks playing a major role in the field of education and culture

330 EUR | JOIN!

SUPPORTING MEMBER

Member states, associations, companies, etc. willing to support our organisation, activities or events

550+ EUR | JOIN!

INDIVIDUAL MEMBER

Is accepted on ad hoc basis for former ENCATC members, artists, researchers, trainers and cultural managers not currently affiliated to any institution or organisation. Students are also eligible under this category

330 EUR / STUDENT 50 EUR | JOIN!

ENCATC thanks its members and partners for their collaborations to this issue of the Cultural Policy Tracker!

ENCATC The Cultural Policy Tracker is a quarterly publication gathering contributions from the members of the Think Tank and widely disseminated to policy makers.
Our contributors are leading academics, researchers, experts, practitioners, and policy makers. They are recognised by the industry we belong to as influencers. For our publication, they are generously providing us with high-quality content, commentary, the best industry practices, and personal stories. Their contributions aim to help ENCATC to achieve its mission of helping the cultural sector become stronger and more sustainable. **This publication is made possible thanks to the financial support of the Creative Europe programme of the European Union.**

ENCATC CULTURAL POLICY TRACKER ISSUE N°13
PUBLICATION DATE: August 2026

PUBLISHER: ENCATC, The European network on cultural management and policy, Avenue Maurice 1, 1050 Brussels, Belgium

Editor: GiannaLia Cogliandro Beyens

AUTHORS: Filippo Bagni, Emanuele Bellini, Giovanna Di Mauro, Luciana Lazzeretti, Mika (Jaeyun) Noh, Elena Raevskikh.

Coordinator: Francesca Greppi

Creative Director: Nerina Finetto

Layout Design & Production: Davide Faggiano

CONTACT: T +32 (0)2 201 29 12 WEBSITE: www.encatc.org

FOLLOW US:

SUBSCRIPTION: ENCATC Magazine is produced for ENCATC members and followers. Subscribe to our mailing list.

CARBON FOOTPRINT
Thank you for reading the electronic ENCATC Magazine. Your support is important for helping ENCATC's actions to reduce our carbon footprint.

ENCATC IS THE LEADING EUROPEAN NETWORK ON CULTURAL MANAGEMENT AND POLICY.

It is an independent membership organisation gathering over 100 higher education institutions and cultural organisations in over 40 countries. ENCATC was founded in 1992 to represent, advocate and promote cultural management and cultural policy education, professionalise the cultural sector to make it sustainable, and to create a platform of discussion and exchange at the European and international level.

ENCATC holds the status of an NGO in official partnership with UNESCO, of observer to the Steering Committee for Culture of the Council of Europe, and is co-funded by the Creative Europe programme of the European Union.

CONTACT

T +32 (0)2 201 29 12

info@encatc.org

www.encatc.org

ADDRESS

Avenue Maurice 1

1050 Brussels,

Belgium

ENCATC

Co-funded by the European Union