A Path Towards an Internet of Things and Artificial Intelligence Regulatory Framework

Suada Hadzovic, Sasa Mrdovic, and Milutin Radonjic

The authors research existing initiatives related to establishing the IoT and AI regulatory and legislative framework in the EU and its applicability in developing countries.

Digital Object Identifier: 10.1109/MCOM.002.2200373

Abstract

As technology is the driver of the economy, it is necessary to follow emerging technological trends and to create appropriate conditions for its adoption and implementation as a human-centred technology. In this regard, rules and standards for the Internet of Things (IoT) and Artificial Intelligence (AI) should be established to best use the benefits of technology and to prevent or minimize the consequences of technology misuse. The fifth industrial revolution (Industry 5.0) has already begun, although Industry 4.0 is still developing. Consequently, the original attention has shifted from IoT to AI, with the IoT debate now being a prerequisite for the AI debate. As AI is transforming our lives, a growing number of countries have considered or already adopted national AI strategies. However, in many developing countries, national AI strategies and initiatives for establishing AI and IoT regulation and legislation frameworks yet need to be discussed. The subject of this article is the research of existing initiatives related to establishing the IoT and AI regulatory and legislative framework in the EU and its applicability in developing countries.

Introduction

The Internet of Things (IoT) is a network of connected physical and virtual things that communicate with each other. In IoT, data is created, aggregated, sent across a network, stored, managed, and analyzed to provide helpful information that defines further actions. IoT is characterized by a complex chain of things communicating and working through different infrastructures. The infrastructures extend across countries, sectors, and areas, with numerous stakeholders and their various dynamic relationships and roles. In this regard, it is necessary to determine who is responsible or who will ensure security, data protection, safety, privacy protection, and other issues, all inseparable from AI and IoT.

Artificial Intelligence (AI) is a field of computer science, and it dates to 1943. There is a Traditional AI (Non-Learning), a rule-based AI, and a Modern AI (Learning), a data-based AI.

AI can be interpreted as an umbrella term for techniques of creating intelligence artificially, thus enabling machines to imitate human behaviour. Machine Learning is a subset of AI, and Deep Learning is a subset of Machine Learning. The orientation is towards Deep Learning, thanks to more and better data, more intelligent algorithms, and more powerful hardware with computing power and parallel processing.

AI can be beneficial to humanity, bringing prosperity and well-being. Still, at the same time, there are rising concerns related to privacy, AI replacing human jobs, manipulation by AI, security, and many other issues.

Although IoT and AI can exist stand alone, they enter into a symbiotic relationship. There is a growing trend in which AI complements IoT by adding human-like awareness and decision-making, finally converging towards Artificial Intelligence of Things (AIoT).

Recognizing IoT and AI significance and considering that IoT plays an increasingly important role in data provision to data-based AI, while AI unlocks the IoT potential, we focus on identifying the path towards IoT and AI regulatory framework.

In the case of IoT and AI, traditional telecommunication regulation is most often irrelevant. According to the International Telecommunication Union (ITU), collaborative regulation, or the fifth-generation regulation (G5), is the highest level of a regulatory framework. The G5 regulation is human-centred, with the significant cooperation of regulatory agencies and numerous stakeholders in developing a harmonized approach across sectors that rely on ICT. Data on existing regulations in 2020, published by ITU ICT-Eye and ICT Data Portal, indicate that only 22.05% of countries have IoT/M2M (M2M — Machine to Machine) regulatory framework in place, which means that the IoT regulatory framework is lacking in many countries [1].

The need for a multistakeholder approach is being recognized by increasing initiatives, such as the Global Partnership on Artificial Intelligence (GPAI), aiming to foster responsible AI development. The GPAI members are committed to the five complementary principles outlined in the "OECD Recommendation on Artificial Intelligence" (OECD — Organisation for Economic Co-operation and Development). These five values-base principles are:"inclusive growth, sustainable development, and well-being; human-centred values and fairness; transparency and explainability; robustness, security, and safety; and accountability."

In addition to participation in global partnerships on AI, bilateral partnerships are also pres-

Suada Hadzovic is with the Communications Regulatory Agency, Bosnia and Herzegovina; Sasa Mrdovic is with the University of Sarajevo, Bosnia and Herzegovina; Milutin Radonjic is with the University of Montenegro, Montenegro.

ent. Parallel to participation in the GPAI, the UK and the USA have a cooperation agreement on AI research and development to increase collaboration toward mutual prosperity, security, and well-being.

There are many prominent initiatives worldwide, but our focus would be on the EU's aim to act as a global standard setter on AI policy which aligns with its "Europe fit for the digital age — Roadmap for becoming a global leader." This aim begins to be realized through the AI Act proposal, as the world's first-time attempt to enact a horizontal regulation of AI. While there are discussions to extend the scope of the current AI Act proposal to "general purpose AI" and not limit it to "high-risk AI," others consider that AI and data legislations impede innovation.

We focus on the applicability of EU initiatives in EU candidate and potential candidate countries, and other developing countries striving to build a human-centred regulatory IoT and AI environment.

AI Related Instruments

The advances of IoT and AI have transformed society with the potential to promote the prosperity of human beings and human rights. Still, at the same time, there is a concern about their potential negative impact. In this regard, it is of ultimate importance to establish an IoT and AI regulatory framework that will ensure that human rights and fundamental freedoms are respected, promoted, and protected.

Human Rights Safeguarding and AI Ethics

Generally, existing international human rights instruments remain applicable, including the 2011 UN Guiding Principles on Business and Human Rights, outlining the state's duty to protect human rights and the corporate's responsibility to respect human rights. Regardless of the technology, the Convention for the Protection of Human Rights and Fundamental Freedoms, widely considered the most successful international instrument, remains applicable, together with the Charter of Fundamental Rights of the European Union.

Related to AI, Ad hoc Committee on Artificial Intelligence (CAHAI) examined the feasibility and adopted the document "*Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy, and the rule of law.*" Accordingly, a legal framework for developing, designing, and deploying AI systems needs to contain fundamental principles of protecting human dignity and respect for human rights, democracy, and the rule of law.

UNESCO's Recommendation on the Ethics of Artificial Intelligence is the first international instrument on the ethics of AI adopted by 193 states. It calls for developing regulatory frameworks to achieve accountability and responsibility for the content and outcomes of AI systems, during the whole AI system life cycle.

National AI Strategies

Governments around the world are becoming more aware of the opportunities, but also risks that AI brings. In this regard, there is continuous growth in the number of national AI strategies globally. The 2022 AI Readiness Index indicates that 32,04 % of the 181 ranked countries ranked in 2022 have published national AI strategies, while 8,29 % of the ranked countries are drafting AI strategies. Evidently, continuous development is present, however, global inequality remains as strategies are concentrated in the Global North.

Artificial Intelligence-Related Legislation

On 21 April 2021, the European Commission proposed the first horizontal regulation of AI in the world. On 6 December 2022, the Council of EU adopted its common position (general approach) on the AI Act along with 154 amendments.

Artificial Intelligence Act Proposal: "COM (2021)206 Proposal for a Regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act)" lays down an AI system definition, methodology for risk-based determination, requirements for prohibited and high-risk AI systems, conformity assessment, horizontal obligations, and high-risk AI systems monitoring.

In line with the European Commission's "Better Regulation Agenda" policy, an impact assessment of the AI Act proposal has previously been conducted. According to the impact assessment, the preferred option is a regulatory framework for high-risk AI systems only, where non-high-risk AI systems providers can follow a code of conduct. The assessment estimated the need for 25 officials in institutions for the AI Act implementation.

Aiming to enforce innovation in AI, the AI Act proposal envisages the establishment of a coordinated AI "regulatory sandbox" as a tool that enables companies to research and experiment with new and innovative products, services, or companies under regulatory supervision. A regulatory sandbox allows innovators to test their innovations in a controlled environment, allows regulators to understand the technology better, and encourages consumer choice. The Spanish government presented a pilot for the first AI regulatory sandbox in the EU in 2022. The experience gained will be collected in guidelines, which can be used for future AI regulations.

Aiming to enforce innovation in AI, the AI Act proposal envisages the establishment of a coordinated AI "regulatory sandbox" as a tool that enables companies to research and experiment with new and innovative products, services, or companies under regulatory supervision.

AI Liability Directive Proposal: "COM (2022)496 — Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)" aims to strengthen public trust in AI by introducing rules specific to damages caused by AI systems. Proposed rules deal with the compensation issues for harm by the fault or omission of a developer, provider, or user of an AI system.

IoT and AI pose significant challenges for regulators in their ongoing efforts to provide a balance between protecting consumers, fostering innovation, and addressing potential adverse effects. As rapid technological development brings new services, governments must quickly create, modify, and enforce regulations.

Classification of Related Regulatory and Legislative Landscape in the EU

With the ambition of making the EU a leading role model, a powerful IoT and AI regulatory and legislative framework is formed in the EU. While directives set goals that require EU states to adopt measures to achieve these goals, regulations are binding in all EU states. For simplicity, we have tried to classify the most relevant laws and

The Data Act aims to evaluate intellectual property rights, support business-to-business data sharing, and foster business-to-government data sharing.

regulations, emphasizing that the overview represents only one segment, further complemented by other horizontal, sectoral and industry-specific regulations. All of them build the AI and IoT regulatory framework.

Data-Related Legislation

IoT and AI are accompanied by vast data, which requires adequate data handling. Ensuring the right to privacy and personal data protection has become a more significant challenge than ever, as digital tools can become an instrument of manipulation and abuse. Additionally, as data is the fuel for the digital economy, it is necessary to enable a data-driven innovation by establishing the free flow of data across the sectors and open government data.

General Data Protection Regulation GDPR: Rapid technological development and new ways of data processing have led to the necessary reform of personal data protection in the EU. Thus, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation – GDPR)" established a modern legislative framework governing the data protection and privacy of persons within the EU, and rules regarding the export of data to third countries.

Article 4. of the GDPR defines "personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

By personal data, we can identify individuals, while non-personal data are not related to individuals. Personal data can become non personal data through various techniques such as anonymization, pseudonymization, and encryption.

Data protection principles outlined in the GDPR are "lawfulness, fairness, transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality, and accountability." Data protection by design and data protection by default must be applied from the early beginning i.e. from the IoT design phase.

E-Privacy Directive and draft ePrivacy Regulation: Devices during communication should transfer personal data only if there is a user's consent. "Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive)" is an essential legal instrument for privacy. Based on the need for its reform after 20 years, this directive will be repealed once the final text of the "COM/2017/010 Proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications (draft ePrivacy Regulation)" is agreed upon and adopted.

Free Flow Data Regulation: The GDPR ensures personal data free flow in the EU. In contrast, the non-personal free-flow data is ensured by the "Regulation (EU) 2018/1807 on a framework for the free flow of non/-personal data" which is primarily focused on removing all unjustified requests for localization of data. This regulation facilitates cross-border business, where companies are not obliged to store data in different places and to establish duplicate IT systems.

Open Data Directive: "Directive (EU) 2019/1024 on open data and re-use of public sector information (Open Data Directive)" provides a legislative area determining the minimum requirements for making public-sector information available throughout the EU, focusing on publicly held non-personal data. This directive enhances transparency in the case of public-private agreements involving public sector information, thus avoiding privileged arrangements.

Data Governance Act: Aiming to unlock the re-use of public sector data that falls outside the Open Data Directive, the new legislative focuses on sensitive non-personal (data covered by IP rights) and personal data held by the public sector, respecting the GDPR. In this regard, in line with the 2020 European data strategy, the "Regulation (EU) 2022/868 on European data governance (Data Governance Act" (DGA) provides a horizontal legal ground for improving the establishment of common data spaces and strengthening cross-sectoral data exchange. DGA horizontal measures are relevant for all common data spaces, which are used as instruments to address barriers to the exchange, use, and re-use of data, where sectoral legislation can propose complementary elements specific to the sector.

Data Act Proposal: The second central horizontal legislative after the DGA is the "COM (2022)68 Proposal for a regulation on harmonized rule on fair access to and use of data (Data Act)," which complements the DGA.

The Data Act aims to evaluate intellectual property rights, support business-to-business data sharing, and foster business-to-government data sharing. The Data Act aims to enable users of connected devices to gain access to the data they generate, ensure efficient switching from one cloud data service provider to another, and protect users against illegal data transfers. Also, the Data Act intends to enable the public sector to access and use data held by the private sector necessary for emergencies or the implementation of legal measures. There is also the aspect of protecting small and medium-sized enterprises from unfair conditions in data exchange agreements. Additionally, the Data Act also considers certain aspects of the Data Directive, clarifying that databases containing data from IoT devices and facilities should not be subject to special legal protection, thus ensuring access to databases and the use of data. As expected, the review of "Directive 96/9/EC on the legal protection of databases" and the "Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure" contribute to facilitating the trading and sharing of machine-generated data.

Electronic Communications Related Legislation

Compared to the previous most profitable position of connectivity providers in the traditional telecommunications market, connectivity services are not the most profitable. They account for a relatively low share of total revenue compared to applications and connected devices. Additionally, the IoT connectivity service provider typically does not contract with the end user but with the IoT device provider or service provider. The key challenge is what IoT services fall into the definition of electronic communications services, who is their provider in a complex IoT system, and who is obliged to meet various regulatory obligations such as consumer protection. In the EU, the telecommunications regulatory framework is based on the umbrella document.

Electronic Communications Code: "Directive (EU) 2018/1972, establishing the European Electronic Communications Code (EECC)" is a leading document based on which national regulatory authorities operate. In Article 2 (4) of the EECC, the definition of "electronic communications service" includes under c) 'services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and broadcasting."

To avoid the exhaustion of existing numbering ranges and to find efficient numbering and addressing solutions for M2M communications as a long-term solution, IoT applications should use IPv6 addresses or numbers/addresses other than E.164 numbers [2]. The vast IPv6 address space can satisfy IoT's enormous need for identifiers, offering a future-proof solution [3]. IPv6 use in IoT could also solve the telephone numbers and international mobile subscriber identity (IMSI) number scarcity problem. However, these numbers are still needed for device identification in the mobile network over which IPv6 is running. In addition, many applications and equipment with personal sensor networks do not use IP and use a LAN gateway.

IoT devices need continuous network access regardless of location. As mobile IoT devices from different countries are connected and depend on roaming, it is necessary to ensure IoT mobile connection without excessive international charges for mobile roaming. Customers should be provided with the possibility to change the connectivity service provider. A lock-in issue example is a when the customer must physically change the subscriber identification module (SIM). Instead of physical SIM card replacement, alternative solutions are developed, such as SoftSIM, eSIM, nuSIM, or iSIM.

The government's role in aligning the national spectrum with internationally harmonized band plans is fundamental, as many IoT services rely on spectrum availability. The industries' role is also required to identify which bands need harmonization. If the industry places demand for additional spectrum, such requests may be nominated through processes via ETSI and CEPT. Regulatory authorities must monitor spectrum use and market development appropriately to make spectrum available to support IoT applications [4].

Sometimes, the existing regulatory framework for frequency allocation must be modified. Establishing an efficient spectrum management framework is necessary, knowing the spectrum requirements for different IoT applications. The European Commission has recently implemented decisions to make 900 MHz and 1800 MHz spectrum ready for 5G innovations and to harmonize the spectrum for systems such as Wi-Fi and short-range devices. These activities aim to ensure that the EU radio spectrum policy can respond to the pressure demand for advanced networks [5].

Cybersecurity-Related Legislation

Cybersecurity aims to reduce cyber-attack risk by using technologies, processes, and controls to protect systems, networks, programs, users, devices, and data.

Cybersecurity Act: "Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)" lays down tasks and organizational affairs relating to the ENISA and a cybersecurity certification framework for ICT processes, ICT services, and ICT products. The purpose is to ensure an appropriate level of cyber security and to avoid fragmentation of the internal market concerning the cyber security certification scheme. Article 2 (1) of the Cybersecurity Regulation, defines "cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats."

NIS 2 Directive: On November 2022, the European Parliament adopted "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) repealing Directive (EU) 2016/1148" a modernized framework for cybersecurity risk management measures.

The Cyber Resilience Act Proposal: Aiming to cover connected IoT devices, a new "COM (2022) 454 Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020" lays down the requirements for the design, development, and production of products with digital elements, market surveillance and the obligations towards cybersecurity.

Platforms-Related Legislation

In an ever-changing digital economy, where online platforms operate in multi-sided markets, accompanying rules are much more difficult to define than before. In January 2022, the European Commission published "Final report — sector inquiry into consumer IoT." Most respondents pointed out that the main obstacles are the cost of technology investment and the competitive situation. The findings of the sector inquiry gave insight into the competitive landscape and respondents' concerns regarding access to data and market concentration.

Platform to Business Regulation: "Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services (Platform to Business Regulation)" applies to online search engines and online intermediation services. It focuses on ensuring fairness, transparency, and adequate compensation for business and corporate website users.

Directive on e-commerce: "Directive 2000/31/EC (Directive on e-commerce)" provides the foundational legal framework "on certain legal aspects of information society services, particularly electronic commerce." But, given the digital evolution that has taken place since the introduction of this directive, two regulations based on this primary directive have been recently introduced to respond to new challenges.

In an ever-changing digital economy, where online platforms operate in multi-sided markets, accompanying rules are much more difficult to define than before.

One of the five key areas belongs to digital transformation, which focuses on ensuring that consumers are protected online as much as offline.

Digital Service Act: "Regulation (EU) 2022/2065 on a Single Market For Digital Services (Digital Service Act)" establishes harmonized rules on the provision of intermediary services. Intermediary service means a service such as a "mere conduit" service, a "caching" service, or a "hosting" service. Digital Service Act lays down conditions for the liability exemption of intermediary service providers and rules on specific due diligence obligations adapted to particular categories of intermediary service providers.

Digital Market Act: "Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act)" establishes rules for "Gatekeepers," which are platforms with a powerful influence in the digital market. Through gatekeepers, business users connect with customers so that gatekeepers can be a bottleneck between businesses and consumers. Additionally, gatekeepers can operate as private policymakers and impose unfair conditions. Accordingly, Digital Markets Act aims to prevent this possibility and ensure the openness of critical digital services. This way, Digital Markets Act complements the competition law at the EU and national levels.

All these rules aim to create a digital environment that will encourage competitiveness and innovation and, above all, a safer digital space in which the user's fundamental rights are respected and protected, a prerequisite for human-centred IoT and AI.

Table 1 provides an overview of different competent authorities, showing a need for wide range of competencies.

Consumer Rights Protection Related Legislation

With the new Consumer Agenda 2020-2025, the general strategic framework of EU consumer policy has been updated. One of the five key areas belongs to digital transformation, which focuses on ensuring that consumers are protected online as much as offline. The New Deal for Consumers aims to modernize consumer protection rules, provide better compensation opportunities, improve consumer awareness, ensure equal treatment, and consider future challenges brought by the new economic environment and new technologies.

Omnibus Directive: Following the New Deal for Consumers, the "Directive 2019/2161 as regards the better enforcement and modernization of Union consumer protection rules (Omnibus Directive)" was adopted to update the four consumer protection directives considering digital developments. These four directives' updates concern unfair contract terms, price indications, unfair commercial practices, and consumer rights.

Revision of Product Liability Directive Proposal: "COM (2022) 495 Proposal for a directive on liability for defective products" will repeal Product Liability Directive 85/374/EEC by adapting liability rules to the digital age and artificial intelligence. Because IoT is tied to various products and services and actors involved, assigning liability may be difficult, and product liability directive must be applied to tangible and non-tangible goods, as well as to digital content and digital services.

Sale of Goods Directive: It should be emphasized that "Directive 2019/771 on certain aspects concerning contracts for the sale of goods (Sale of Goods Directive)" classifies goods into two categories where the "goods with digital elements" category incorporate or is interconnected with digital content or digital services in such a way that their absence would prevent the functioning of goods.

Digital Content Directive: Additionally, there is the "Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services" contribution of laying down rules on the compliance of digital content or a digital service with the contract, remedies in the absence of such compliance, and the modification of digital content or a digital service. Such products should be GDPR-compliant, safe, and free from personal security risks and cybersecurity failures.

General Product Safety Regulation Proposal: While liability rules are ex-post rules, product safety rules are ex-ante rules, which are complementary and create an environment that strengthens consumer protection. IoT must meet the essential safety and health requirements ground on sectorial safety legislation and the "COM (2021) 346 Proposal for a regulation on general product safety," complemented by "Regulation (EU) 2019/1020 on market surveillance and compliance of products."

A Path of Three Steps

Every sector will be touched by the IoT and AI, where the outdated or non-existent IoT and AI regulatory framework can be a barrier to long-term market development, well-being enhancement, consumer protection, etc.

We can identify three steps towards IoT and AI regulatory and legislative framework development.

1. *National AI Strategy development — ICT regulator as initiator:* National AI Strategy is a key document for enhancing AI adoption. It needs to be developed according to the assessment of a country's strategic priorities previously undertaking multistakeholder consultations. More than a hundred countries, mainly developing countries, do not have AI Strategy. In this regard, a proactive ICT regulator could be the authority that initiates, raise awareness, and thus encourage national AI strategy development. Common AI strategy blocks are Ethical standards, Investment, Data, Digital Infrastructure, Regulation, International collaboration, Education and AI Skills Development, Scientific Research, Innovation, and Industrialization of AI technologies. Depending on specific objectives and measures of the AI strategy, responsible authorities can differ, from the AI Council, AI Institute, ministries of education, research, ICT, labour, finance, etc.
2. *New IoT and AI regulatory framework development — ICT regulator as coordinating authority:* By integrating AI with data from IoT, the true potential of IoT is enabled. As the ICT regulator has a central part in enhancing innovation and developing the electronic communications market, it could also play a central role in the context of the IoT and AI, following the collaborative regulation model as the latest generation of regulation.

   IoT and AI should be considered from various aspects, which implies that determining the rules requires moving through many overlapping policy areas, such as consumer protection, security, safety, liability, electronic

Legislative	National competent authority	Committee/Board
“COM (2022) 206 Proposal (AI Act Proposal)”	Article 59. Par. 2. a national supervisory authority among the national competent authorities	Article 56. Par. 1. European Artificial Intelligence Board
“COM (2022) 496 Proposal (AI Liability Directive Proposal)”	Article 3. Par 1. National courts	
“Regulation (EU) 2016/679 (General Data Protection Regulation — GDPR)”	Article 51. Par. 1. one or more independent public authorities (Supervisory authority)	Article 68. Par. 3. European Data Protection Board
“COM (2017) 010 Draft ePrivacy Regulation”	Article 18. Par 1. The same supervisory authority as for the GDPR	Article 19 European Data Protection Board
“Regulation (EU) 2018/1807 Free Flow Data”	Article 7. Par 1. A single point of contact	
“Open Data Directive EU (2019) 1024”	Article 4. Par 1. Public sector bodies	Article 16 Committee on open data and the re-use of public sector information
“Regulation (EU) 2022/868 on European data governance (Data Governance Act)”	Article 7. Par 1. one or more competent bodies, which may be competent for particular sectors.	Article 29. Par 1. European Data Innovation Board
“COM (2022) 68 Proposal (Data Act)”	Article 31. Par 1. one or more competent authorities	
“European Electronic Code EU (2018) 1972”	Article 5. National regulatory and other competent authorities.	Article 10. BEREC (the Body of European Regulators for Electronic Communications
“Regulation (EU) 2019/881 (Cybersecurity Act)”	Article 58. Par. 1. one or more national cybersecurity certification authorities	Article 3. ENISA (the European Union Agency for Cybersecurity)
“Directive (EU) 2022/2555 (NIS 2 Directive)”	Article 8. Par. 1. one or more competent authorities for cybersecurity Article 9. Par. 1. One or more cyber crisis management authorities Article 10. Par. 1. one or more CSIRTs.	Article 15. CSIRTs network (Computer security incident response teams) Article 16. European cyber crisis liaison organization network (EU-CyCLONe)
“COM (2022) 454 Cyber Resilience Act Proposal”	Article 25. “Notifying authority” “Conformity assessment body” Article 48. The market surveillance authorities	Article 45. ENISA
“(EU) 2019/1150 (Platform to Business Regulation)”	Article 14. competent national courts	
“Regulation (EU) 2022/2065 (Digital Service Act)”	Article 49. Par 1. one or more competent authorities Article 49. Par 2. Digital Services Coordinator.	Article 61. Par 1. “European Board for Digital Services”
“Regulation (EU) 2022/1925 (Digital Markets Act)”	72) Preamble — competent independent authorities, such as data or consumer protection authorities.	Article 32. Par. 1. Digital Markets Advisory Committee
“Directive (EU) 2019/2161 (The Omnibus Directive)”	Article 13. Par. 3 the competent national authority or court	Article 5. European Consumer Centres Network
“COM (2022) 495 Proposal for a directive on liability for defective products”	Article 8. national court national authorities responsible for the enforcement of consumer protection laws	
“COM (2021) 346 Proposal for a regulation on general product safety”	Article 31. Par 4. the competent authorities on product safety and on surveillance and control	Article 28. Par 1. Consumer Safety Network

TABLE 1. Overview of different competent authorities.

communications, privacy, data protection, and many others. ITU’s concept of most advanced or collaborative regulation refers to ICT regulators’ collaboration with regulators in other sectors. The breadth of collaboration refers to collaboration with authorities on Internet issues, spectrum management, consumer protection, competition, broadcasting, competition, and finance.

Relevant legislation must be future-proof without restrictions on technological development, as it is in the presented EU model. Finally, a new regulatory framework should be prepared and assessed using the Regulatory Impact Assessment (RIA) method to select the best option applicable to the country. Prior to establishing AI national supervisory authority, the ICT regulator is a good candidate for coordinating authority within some form of the advisory committee with representatives from identified competent authorities (data protection authority, ethics committee, cybersecurity responsible authorities, sectoral ministries, etc.).

3. *Multistakeholder governance development — National AI Supervisory Authority as coordinating authority:* IoT and AI require a revised role of regulatory authorities. According to the AI Act Proposal, national competent authorities shall be established or designed by the state; among them, a national supervisory authority shall be designed. Besides governance, involving civil society, the private sector, and academia is crucial for success.

Conclusion

Developed countries are racing to adopt AI, while most developing countries lag.

The AI wave is coming and developing countries can take opportunities brought by AI, with a proactive regulatory approach while respecting, protecting, and promoting human rights.

Failure to take a proactive regulatory approach can lead to unfortunate outcomes as technologies are shaped by our choice.

One proactive approach can be the path towards a human-centred regulatory IoT and AI environment identified in this article, along with its legislative and regulatory building blocks.

References

[1] ITU ICT-Eye, ICT DATA PORTAL, Internet of Things; https://www.itu.int/net4/itu-d/icteye#/topics/2015, accessed on 27th Feb. 2023.

[2] ECC Report 153, Numbering and Addressing in Machine-to-Machine (M2M) Communications, Nov. 2010; https://docdb.cept.org/download/cbdd8141-61c6/ECCREP153.PDF, accessed on 27th Feb. 2023.

[3] ETSI GR IP6 008 V1.1.1 (2017-06); https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_ip6008v010101p.pdf, accessed on 27th Feb. 2023.

[4] BEREC Report on Enabling the Internet of Things, 2016; https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-enabling-the-internet-of-things, accessed on 27th Feb. 2023.

[5] https://digital-strategy.ec.europa.eu/en/news/harmonising-spectrum-enhanced-connectivity-ready-5g-and-innovation, accessed on 27th Feb. 2023.

Biographies

Suada Hadzovic [M] (shadzovic@rak.ba) is an Expert Advisor with the Communications Regulatory Agency. She is currently pursuing her Ph.D. thesis at the Faculty of Electrical Engineering, University of Sarajevo. Her research area is focused on regulatory aspects of IoT and AI.

Sasa Mrdovic [M] (sasa.mrdovic@etf.unsa.ba) is a Professor at the Faculty of Electrical Engineering, University of Sarajevo. He earned his Ph.D. in 2009. His current research interests are the security of IoT networks and forensics. He teaches courses on computer networks and security.

Milutin RadonjiC [M] (mico@ucg.ac.me) is a Professor at the University of Montenegro, Faculty of Electrical Engineering. He earned his Ph.D. in 2011. His key research and expertise include packet switching systems, computer networks, IoT systems, and digital system design.