1

The EU IoT Policy and Regulatory Strategy – the Way Forward

Nikolaos Isaris

European Commission, Belgium

1.1 Introduction

Already in the Digitising European Industry (DEI) strategy [1], the Commission set up the ambitious goal of making Europe the world leader in the Internet of Things (IoT).

In 2017, we launched five IoT Large-Scale Pilot (LSP) projects [2] in the areas of smart cities, health, wearables, cars and food and agriculture, with a total amount of EU funding of 100 million EUR. In 2018, a set of eight IoT security and privacy research projects was launched with a budget of 37 million EUR. In 2019, six additional LSP projects (two on agriculture, one on energy and three on digital health and care) have been launched. These pilot deployment projects are addressing both the technology aspects and the regulatory and societal issues around IoT, demonstrating that IoT technology and digitisation have the potential of solving societal challenges as well as stimulating the creation of open European and global standards.

However, these research and innovation activities need to be taken in parallel with the relevant policy and regulatory steps, which can contribute to the delivery of our goals. The current work that the Commission is undertaking on the legal framework for liability for emerging digital technologies, should help to stimulate investment and to enhance users' trust in them, especially for IoT and Artificial Intelligence (AI). In addition, the recently adopted ICT Cybersecurity Certification Framework will enable the development of IoT innovation, while providing security at the expected level of assurance.

However, the next Commission will need to be able to face the bigger challenge of European businesses' contribution to the global digital supply chain. Despite the fact that the region remains one of the world's largest markets for digital products and services, Europe is increasingly dependent on foreign technologies in key parts of its economy. The risk is that the next digital transformation wave will be entirely shaped by third countries.

The current chapter aims to explain the importance of the right policy and regulatory strategy to overcome the challenges in the next decade.

1.2 Safety and Liability for Emerging Digital Technologies

Emerging digital technologies, such as IoT and AI, will create new opportunities for our economy and society. The increased autonomy of the products and services incorporating emerging digital technologies will result in beneficial effects, in particular in terms of increased productivity, positive societal outcomes, prevention of human error and potentially improved safety. For example, a home equipped with sensors, robots and connected devices enables elderly people to live in their homes safely and independently. This smart environment can monitor their health status and prevent them from becoming frail, as well as keeping them remotely in touch with their doctor. In another application area, precision farming, these technologies promise to reduce pesticide use and increase yields.

However, certain characteristics of emerging digital technologies bring new challenges concerning safety and liability. The complexity of these technologies is reflected on both the plurality of actors involved in the value chain and the multiplicity of components, parts, systems or services, which together form a joint ecosystem. The vast amounts of data involved and the reliance on algorithms make it more difficult to understand the potential causes of damage. In addition, the increased autonomy makes it more difficult to predict the behaviour of the product compared to the functions that were attributed initially by the producer. Finally, connectivity can also expose the products to cyber-threats.

Therefore, the challenge is to assess whether the EU and national legal frameworks on safety and liability are able to cope with the challenges brought by these technologies. Ensuring safety in a connected world is primordial. Moreover, safer products mean less need for liability actions. There is a need for clear, predictable and interoperable legal frameworks able to address the new technological challenges, in order to guarantee trust for all

users, while encouraging continuous innovation and providing a level playing field for the industry.

The Commission Staff Working Document on Liability for emerging digital technologies [3] kicked off a first assessment of liability issues. As a follow-up, the Expert Group on Liability and New Technologies [4] was created, in order to provide the Commission with expertise on the applicability of the Product Liability Directive 85/374/EEC and with assistance in developing guiding principles for possible adaptations of applicable laws related to new technologies.

The Communication on Artificial Intelligence for Europe [5] announced that in 2019 the Commission would publish two deliverables:

- A guidance document on the interpretation of the Product Liability Directive in light of technological developments; and
- A report on the broader implications for, potential gaps in and orientations for, the liability and safety frameworks for AI, IoT and robotics.

The aim is to ensure legal clarity for consumers and producers in case of defective products, to facilitate the uptake of emerging digital technologies and to ensure users' trust and protection.

1.3 Cybersecurity Certification for IoT Products, Services and Processes

IoT implementation comes with a number of challenges, the most important of which are: security, privacy, data protection, increasing trust and consumer acceptance in IoT. Some of the challenges are due to the increased scale and scope of IoT with billions of devices potentially connected to the Internet. This number may pose a commensurate number of security risks.

In addition, IoT brings along new types of concerns on top of the safety aspects that exist in any consumer product or service. Moreover, the life cycle of some of the connected devices varies considerably and this can be a source of additional complexity when clarifying questions of security, upgradeability, liability and others. Finally, as the recent cyber-attacks have shown, consumer IoT vulnerabilities can be the source of damage in critical infrastructures and industrial IoT.

That is why the Cybersecurity Act [6], which entered into force on 27 June 2019, established the European cybersecurity certification

framework, putting forward the instruments that will allow the development of IoT innovation. Cybersecurity certification will become less expensive, more effective and commercially attractive.

The main thrust of the legislation is establishing clear rules and a governance framework that would allow to set up European schemes for the cybersecurity certification of ICT products, services and processes. The framework allows also the potential development of labels accompanying a specific scheme. This would allow, for example, the creation of a Trusted IoT label for a particular type of IoT products, services or processes.

As next steps according to the Cybersecurity Act, the Commission needs to set up the governance framework and set out the policy priorities for the future. The 2017 Communication that accompanied the Cybersecurity Act indicated three priority areas for certification schemes: (1) IoT, (2) critical or high-risk applications, and (3) security products, networks, systems and services (e.g. VPNs, firewalls). Other technologies, including 5G, have also made the priority list since then.

Therefore, the 'Union rolling work programme for European Cybersecurity Certification' is a forward-looking document which shall identify strategic priorities for future schemes. In particular, the rolling work programme will include a list of ICT products, services and processes or categories thereof that may benefit from being included in the scope of a European Cybersecurity Certification Scheme.

In the context of the ongoing work on liability in emerging digital technologies, certification could be also used to demonstrate that the required standard of care has been met by manufactures of ICT products or providers of ICT services.

1.4 Globally Competitive European Digital Supply Chains for the Next Generation Internet

Emerging digital technologies and services such as AI, 5G, IoT or edge computing are transforming many economic sectors significantly (e.g. health/care, manufacturing, agriculture, smart cities, energy, mobility). They are creating new markets with enormous potential. However, Europe currently still depends on foreign technologies for key parts of the digital supply chain. In essence, while connectivity infrastructure is mostly European, the necessary hardware and software is often made elsewhere. This technological dependence could translate into dependence for the next wave of data solutions: there is a risk that Europe will become a simple consumer of products and services made elsewhere.

This concerns mainly investments and rapid deployment of connectivity and data infrastructure, as well as accompanying policy measures required to create the right conditions for scalable and viable business models as well as critical mass of investments.

Europe is particularly exposed to substantial global competition and market concentration by foreign players in the field of cloud infrastructure and telecom networks supply, which may adversely affect its position for the Next Generation Internet, in particular concerning 5G, IoT and cloud services. A 'do nothing' option would only serve to increase the global imbalance, will foster the dominance of a few global non-European players and let Europe drift further behind, with negative consequences in terms of growth and undesired global dependencies for critical components, technologies and infrastructures.

If Europe really wants to become a global leader in IoT in the near future, it is crucial to look at connecting IoT ecosystems across different sectors, to continue supporting piloting and testbeds at scale and to check whether the regulatory and policy framework across different policy aspects are fit for purpose.

This is why the way forward is to focus on how data is gathered, managed and shared across the European Union and internationally, rather than looking into a full harmonisation of IoT services. Globally there are major players battling to control the supply and delivery of future digital products and services which will be ever more critical for the proper functioning of our society and economy. Europe is, therefore, at a crossroad in terms of ensuring freedom of choice and promoting values such as user control, ethics, privacy and security embodied in the future digital solutions. This requires new partnerships cutting across traditional value chains, which were formed during the first phases of digital transformation with the emergence of the Internet.

The Commission has proposed as part of the new Horizon Europe programme to explore the idea of a partnership on Smart Networks and Services, bridging the major connectivity and service infrastructures required for the Next Generation Internet, including 5G/6G, Internet of Things and distributed Cloud Computing.

Such a partnership would be driven by industrial agendas and coordinated with the EU Member States. This kind of endeavour requires that all relevant stakeholders react to this idea and formulate together the best way of partnering to ensure that Europe can continue to play a prominent role in taking the IoT and digital transformation forward into the next decade.

1.5 Conclusion

We must now build on top of the achievements of the Digitising European Industry (DEI) strategy, and the policy and regulatory strategy mentioned above. The European Union should strive for, and promote internationally, a third way of doing digital policy that is human-centric and founded on respect for fundamental rights, distinct from both a *laissez-faire* approach, privately ruled digital economy and society, and a top-down controlled model. This third way will enhance trust, promote an inclusive digital society and become a competitive advantage for European companies acting worldwide. It will allow Europe to create economic value in accordance with its core values.

References

[1] Digitising European Industry, online at: https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry

[2] IoT European Large-Scale Pilots, online at: https://european-iot-pilots.eu/

[3] Commission Staff Working Document on Liability for emerging digital technologies SWD/2018/137, online at: https://ec.europa.eu/digital-single-market/en/news/european-commission-staff-working-document-liability-emerging-digital-technologies

[4] Expert Group on Liability and New Technologies. Register of Commission Expert groups online at: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592

[5] Communication on Artificial Intelligence for Europe COM(2018)237, online at: https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 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), PE/86/2018/REV/1, OJ L 151, 7.6.2019, p. 15–69, online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561545219894&uri=CELEX:32019R0881