

The Challenge of Regulation in the Face of New Technologies: From the Dawn of the Internet to the Age of Artificial Intelligence

Lecturer **Bogdan Cristian TRANDAFIRESCU**¹

Abstract

The article analyzes the relationship between technological innovation and the legislator's response, as well as the capacity of law to adapt to new realities. It compares the now historical experience of regulating legal relationships in the digital environment with the current challenges generated by artificial intelligence. The paper is structured in two main parts, followed by conclusions. The first part examines the beginnings of the Internet and the evolution of the regulations it required. The second part analyzes artificial intelligence as a new object of regulation. The analysis compares the main regulatory models developed in the European Union, the United States of America, and China. What brings these two technological eras closer together is their radical novelty in relation to the traditional legal relationships and institutions with which law has operated for millennia, as well as the question of the legislator's response. What distinguishes them is the fact that, whereas the Internet is merely a virtual environment in which people interact and for which old legal institutions were adapted, artificial intelligence appears rather as a reactive reality with which one can interact, which acts, which will become increasingly independent, and which may perhaps acquire self-awareness in the more distant future.

Keywords: internet regulation; artificial intelligence; electronic commerce; electronic signature; legal liability; technological neutrality; the ethics of artificial intelligence

JEL Classification: K10, K24

DOI: 10.62768/PLPA/2026/15/2/04

Please cite this article as: Trandafirescu, Bogdan Cristian, „The Challenge of Regulation in the Face of New Technologies: From the Dawn of the Internet to the Age of Artificial Intelligence”, <i>Perspectives of Law and Public Administration</i> 15, no. 2 (June 2026): 237-252.	Article History Received: 25 February 2026 Revised: 27 April 2026 Accepted: 25 May 2026
---	---

1. Introduction

Technology has always brought about transformations and developments of positive law. Printing weakened the old monopolies, industrialization necessitated the birth of labour law, and nuclear energy led to the emergence of special international (treaty-based) and national regulations. Such was the Internet in the recent past, and such is artificial intelligence today; both are technologies that cannot be integrated into the existing normative framework, both compel the legislator to adapt the law to new

¹ Bogdan Cristian Trandafirescu - Faculty of Law and Administrative Sciences, Ovidius University of Constanța, Romania, <https://orcid.org/0009-0004-2113-0485> bogdan@aaيدا.ro.

realities.

The Internet emerged in the final decades of the twentieth century. The first online contractual relationships were treated through the instruments of the common law, which generated difficulties regarding consent, contract formation, and consumer protection. Regulation came late and in a fragmented manner, more as a reaction, always lagging behind technological development.

Today, with the rise of artificial intelligence, the law is confronted with a challenge of a different order. If the Internet merely transferred already known legal relations into the digital environment, artificial intelligence brings autonomous decisions, the active involvement of software capable of understanding and acting within legal relations, concrete legal effects, and diffuse responsibilities.

The fundamental question from which we begin is the following: can the law learn from the delays and incomplete solutions of Internet regulation and, this time, build an adequate and anticipatory normative framework, capable of preventing risks and protecting fundamental values? Or will artificial intelligence, by the radical nature of its novelty, once again succeed in taking the legislator by surprise, even to a greater extent than the Internet did in the past?

In order to attempt to answer this question, in our undertaking we shall first analyse the evolution of Internet regulation (which has already entered history), then the specific challenges of artificial intelligence, and, finally, we shall place the two technological eras in parallel in order to draw the conclusions that will be required.

2. The Pioneering Period of the Internet and the First Digital Legal Relations

2.1. The Birth and Development of the Internet

The Internet has its origins in the ARPANET project (Advanced Research Projects Agency Network), launched in 1969 by the United States Department of Defense – Advanced Research Projects Agency (ARPA), for military and academic purposes².

The development of the TCP/IP protocols in the 1970s and the expansion of funding through the National Science Foundation (NSFNET) in the 1980s transformed the network into a global infrastructure. The decisive moment was the invention of the World Wide Web by Tim Berners-Lee in 1991, which introduced the graphical browser interface and facilitated public access to information³. The 1990s brought about the commercialisation of the Internet and the first applications with social and economic impact: e-mail, commercial websites, search engines, and electronic commerce⁴. The

² Vinton G. Cerf and Robert E. Kahn, "A Protocol for Packet Network Intercommunication," *IEEE Transactions on Communications* 22, no. 5 (1974): 637–648, <https://doi.org/10.1109/TCOM.1974.1092259>.

³ Tim Berners-Lee, with Mark Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor* (San Francisco: HarperSanFrancisco, 1999), 27–54.

⁴ Janet Abbate, *Inventing the Internet* (Cambridge, MA: MIT Press, 1999), 43–68.

Internet appeared to be an unregulated space.

Governments and international organizations could not ignore this new reality and began to formulate the first attempts at regulation.

2.2. The First Digital Legal Relations

Distance contracts constituted the first type of digital legal relation. The question arose whether a click or an e-mail message could produce binding legal effects; this revived the older doctrinal debate regarding the theories of the moment of contract conclusion (the theory of dispatch, transmission, receipt, information)⁵.

The first issue was that of the legal status of the convention (agreement of wills) concluded in the digital environment. The obvious solution was the equation of electronic documents with those on paper, and of the handwritten signature with the electronic signature – Model Law on Electronic Commerce (1996) and Model Law on Electronic Signatures (2001), adopted by the United Nations Commission on International Trade Law (UNCITRAL).

Also, during this period, concerns arose regarding consumer protection in the conclusion of distance contracts, themes that would first be reflected in soft-law instruments and later in European directives subsequently transposed into the legislation of the Member States.

2.3. The Legislator's Reaction – A Model of Normative Staging

The emergence of the Internet generated a gradual reaction from the “world of law,” which may be seen as a model of adaptation to new technologies.

UNCITRAL adopted the Model Law on Electronic Commerce (1996) and the Model Law on Electronic Signatures (2001), consecrating for the first time notions such as electronic document, data message, and electronic signature, and affirming the principle of functional equivalence.

The Organisation for Economic Co-operation and Development (OECD) issued in 1999 the Guidelines for Consumer Protection in the Context of Electronic Commerce, consecrating transparency of information, the right of withdrawal, and the protection of minors.

The International Chamber of Commerce (ICC) issued in 1996 the ICC Guidelines on Advertising and Marketing on the Internet (revised in 2003), which establish standards of transparency and fairness for traders in the online environment. During the same period, the ICC also published the ICC General Usage for Internationally Contracted Electronic Transactions and adapted the ICC Code of Direct Marketing (1998) to the electronic environment, thus providing a set of rules of conduct for digital marketing and consumer protection.

⁵ Maria Căzănel and Sorin Calafus, “The Notions of Parties, Third Parties and Successors in Title in Contractual Relations,” in *5th International Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM 2018*, vol. 18, book 1.6 (2018), 302, <https://doi.org/10.5593/sgemsocialF2018/1.6/S02.037>.

The Asia-Pacific Economic Cooperation Forum (APEC) adopted in 1998 the APEC Blueprint for Action on Electronic Commerce, by which member economies undertook to create an environment favourable to the development of electronic commerce, based on self-regulation and common technical standards. In 2004, APEC also adopted the APEC Privacy Framework, which sets out principles for the protection of personal data in cross-border information flows.

International conventions. The Council of Europe adopted in 2001 the Convention on Cybercrime (Budapest), the first binding international instrument in the digital field.

The World Intellectual Property Organization (WIPO) adopted in 1996 the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, thereby extending copyright protection into the digital environment.

In 2005, the Hague Conference on Private International Law adopted the Convention on Choice of Court Agreements, with direct impact on disputes generated by international electronic contracts.

European Union directives laid the foundations of the European law of the information society, creating an innovative legal regime and consecrating the limitation of intermediary liability (safe harbour):

- Directive 97/7/EC on the protection of consumers in respect of distance contracts⁶;
- Directive 1999/93/EC on electronic signatures⁷;
- Directive 2000/31/EC on electronic commerce⁸.

National legislation. Across the world, laws were adopted regarding electronic commerce, electronic signatures, and consumer protection. In Romania: Law no. 455/2001 on electronic signatures⁹, Law no. 365/2002 on electronic commerce¹⁰, and Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector marked the transition to a digital legal order¹¹.

The reaction of the law to the emergence of legal relations in the virtual environment followed a relatively coherent path: the academic environment was the first to perceive the need for special regulation, initiating debates (conferences, published scientific works, etc.); the second stage was represented by the adoption by

⁶ Directive 97/7/EC of the European Parliament and of the Council of May 20, 1997, on the protection of consumers in respect of distance contracts, *Official Journal of the European Communities* L 144 (June 4, 1997): 19–27, <https://eur-lex.europa.eu/eli/dir/1997/7/oj>.

⁷ Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999, on a Community framework for electronic signatures, *Official Journal of the European Communities* L 13 (January 19, 2000): 12–20, <https://eur-lex.europa.eu/eli/dir/1999/93/oj>.

⁸ Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *Official Journal of the European Communities* L 178 (July 17, 2000): 1–16, <https://eur-lex.europa.eu/eli/dir/2000/31/oj>.

⁹ Law No. 455/2001 on the electronic signature, Official Gazette of Romania, Part I, No. 429 of 31 July 2001.

¹⁰ Law No. 365/2002 on electronic commerce, Official Gazette of Romania, Part I, No. 483 of 5 July 2002.

¹¹ Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, Official Gazette of Romania, Part I, No. 1101 of 25 November 2004.

international organizations of soft-law instruments; the third stage was represented by the adoption of international conventions and European directives, whose regulatory solutions were transposed (sometimes in an even more elaborate manner) into national legislation. This process, although in essence reactive, gradually led to the formation of a coherent and stable normative framework.

This experience today constitutes a historical benchmark for the adaptation of the law to new technologies and offers a point of support for reflection upon the regulation of artificial intelligence.

3. Artificial Intelligence – The New Frontier of Legal Challenges

3.1. Definition and Conceptual Difficulties

The notion of “artificial intelligence” does not yet have a unanimously accepted definition¹².

Doctrine and technological practice generally distinguish between two categories:

- narrow AI, which performs well-defined tasks (facial recognition, automatic translation) but does not possess the ability to interact within relations of a social nature and does not go beyond the limits of its programming;
- generative AI, which uses complex neural-network-type models to produce new content (texts, images, sounds, code), in a manner that is difficult to anticipate and at least apparently spontaneous.

Whereas narrow AI can easily be fitted within existing/traditional legislation (product liability, consumer protection, regulation of personal data), generative AI raises fundamentally new issues: who is the author of a work generated by AI, who is liable for a decisional error?¹³

An official and comprehensive definition is proposed by the European Commission’s High-Level Expert Group on AI (2019) – “artificial intelligence designates systems which, on the basis of an analysis of the environment, are capable of making decisions with a certain degree of autonomy in order to achieve predetermined objectives”¹⁴. This definition has the merit of establishing a fundamental criterion on the basis of which the distinction may be made between simple computer software and genuine artificial intelligence, namely functional autonomy.

¹² Brent Mittelstadt, Chris Russell, and Sandra Wachter, “Explaining Explanations in AI,” in *Proceedings of the Conference on Fairness, Accountability, and Transparency* (New York: Association for Computing Machinery, 2019), 279–288, <https://doi.org/10.1145/3287560.3287574>.

¹³ Ryan Calo, “Artificial Intelligence Policy: A Primer and Roadmap,” *UC Davis Law Review* 51, no. 2 (2017): 403–405, <https://lawreview.law.ucdavis.edu/archives/51/2/artificial-intelligence-policy-primer-and-roadmap>.

¹⁴ High-Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Scientific Disciplines* (Brussels: European Commission, 2018), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341.

3.2. The Break with the Internet

Comparing artificial intelligence with the Internet highlights the different nature of the two. The Internet (in itself) merely mirrors physical reality in parallel; it is only a virtual space in which social relations may unfold. In this space, human subjects are the ones who act, create content, conclude juridical conventions that may be fitted within traditional legal institutions (distance sale, advertising, communication, dissemination of protected works). Over time, the Internet has become an integral part of individuals (natural or legal persons) access to state institutions and of the exercise of certain fundamental rights¹⁵. The legislator merely had to adapt pre-existing institutions to a new technical environment.

Artificial intelligence raises completely new legal issues. AI acts as a decision-making subject: it selects, filters, and even produces autonomous outputs whose internal logic is, in many cases, inaccessible even to its developers. This opacity (known as the “black box problem”) calls into question the application of traditional legal notions such as will, the juridical act, and fault¹⁶.

Intelligence has the vocation of becoming an actor in the legal relation (a situation already actual, not merely potential) and coexists alongside man in the virtual space of the Internet. This time, the legislator must not merely adapt old institutions to a virtual reality (as it did with regard to the Internet), but must adopt legislation of a different nature; we may speak of a genuine legal revolution.

4. Models of AI Regulation at Global Level

Artificial intelligence has gone beyond the experimental stage in software laboratories; it is already a globally integrated presence in today’s world, and its effects are systemic and profound. We are living through a genuine technological revolution that will certainly enter history alongside the other major leaps in the history of humankind (the appearance of agriculture, printing, the industrial revolution). States, indeed humanity as a whole, cannot afford to remain indifferent to the evolution of AI; the intervention of the legislator is necessary and inevitable.

4.1. From Soft-Law Principles to Binding Rules

In a manner similar to the regulation of the Internet, the first reactions to the challenges of AI took the form of soft-law documents, which prepared the ground for rules of positive law.

In 2019, the Organisation for Economic Co-operation and Development (OECD) adopted the Recommendation of the Council on Artificial Intelligence, the first

¹⁵ Daniel-Mihail Șandru, “Prolegomena on the Right to the Internet,” *Law Review* 15, no. 1 (2025): 32–41, <https://internationallawreview.universuljuridic.ro/index.php/journal/article/view/443>.

¹⁶ Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 6–7.

intergovernmental instrument in the field¹⁷. The document is organised on two levels: a) five value-based principles for trustworthy artificial intelligence and b) five recommendations addressed to states, concerning the public policies and international cooperation necessary for the implementation of the former.

The 5 value-based principles are:

- inclusive growth, sustainable development and well-being;
- respect for the rule of law, human rights and democratic values, including fairness and privacy;
- transparency;
- robustness, security and safety;
- accountability.

The 5 recommendations addressed to states are:

- investments in research and development in the field of artificial intelligence;
- promoting an ecosystem favourable to artificial intelligence;
- shaping an interoperable governance and public policy framework favourable to AI development;
- developing human capacity and preparing for the transformation of the labour market;
- international cooperation for trustworthy artificial intelligence.

Both the principles and the recommendations consecrate the idea of an AI gravitating around the fundamental principles of law¹⁸ and the fundamental rights of man.

In 2021, UNESCO adopted the Recommendation on the Ethics of Artificial Intelligence, a document ratified by 193 states¹⁹. The Recommendation provides principles for the ethical governance of AI, including the prohibition of mass biometric surveillance, users' right to explainability, protection of vulnerable groups, and the obligation to carry out human-rights impact assessments before the deployment of high-risk systems.

These documents constituted the starting point for positive-law regulations (normative acts), centred upon the idea that AI must be governed "in the interest of humanity."

4.2. Comparative Law Study

The European Union model – the AI Act and related legislation. The European Union is a pioneer in adopting a legal framework for artificial intelligence. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June

¹⁷ OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, adopted May 22, 2019, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.

¹⁸ For the fundamental principles of law, see Bogdan Cristian Trandafirescu, *Teoria generală a dreptului. Curs universitar [General Theory of Law: University Course]* (Bucharest: Universul Juridic, 2025), 52–57.

¹⁹ UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, adopted November 23, 2021 (Paris: UNESCO, 2021), <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

2024 laying down harmonised rules on artificial intelligence (known as the “Artificial Intelligence Act” or the “AI Act”)²⁰, establishes the first general and binding normative act dedicated to artificial intelligence.

The Regulation classifies AI systems into four categories:

- Systems posing an unacceptable risk – expressly prohibited (social scoring implemented by public authorities, subliminal manipulation of human behaviour, real-time biometric recognition in public spaces, subject to strictly provided exceptions);
- High-risk systems – conditionally permitted, but subject to strict obligations for providers: governance of training data, technical documentation, traceability, ex-ante conformity assessments, human oversight, incident-reporting mechanisms;
- Limited-risk systems – required only to ensure transparency (informing the user that they are interacting with AI);
- Minimal-risk systems – no additional obligations.

Through the AI Act, the European Artificial Intelligence Board is established, which coordinates implementation in the Member States, and sanctions are provided for of up to EUR 30 million or 6% of the operator’s global turnover, following the GDPR model.

In parallel, the Parliament and the Council of the EU proposed the AI Liability Directive, which establishes a presumption of causality in favour of the victim, in order to overcome the evidentiary difficulties generated by algorithmic opacity (the difficulties in determining with precision the logical processes that led to a particular decision, to what extent the decision was in fact determined by the developer’s software or whether there are other factors)²¹.

The revision of the Product Liability Directive extends strict liability to software producers and providers of updates, thus recognising the dynamic character of digital products²².

The United States of America. There is no uniform federal framework, sectoral regulations and soft-law instruments being preferred.

At federal level, the White House published in 2022 the Blueprint for an AI Bill of Rights – a programmatic document setting out five principles: the right to safe and effective systems, protection against algorithmic discrimination, protection of privacy, transparency of automated decisions, and the possibility of human intervention in case

²⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act), *Official Journal of the European Union* L 2024/1689 (July 12, 2024), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

²¹ European Commission, *Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)*, COM(2022) 496 final, 2022/0303(COD) (Brussels, September 28, 2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>.

²² Directive (EU) 2024/2853 of the European Parliament and of the Council of October 23, 2024, on liability for defective products and repealing Council Directive 85/374/EEC, *Official Journal of the European Union* L 2024/2853 (November 18, 2024).

of errors²³. The nature of this act, as well as the principles set out therein, are reminiscent of the Recommendations developed within the OECD (2019).

In 2023, the National Institute of Standards and Technology (NIST) published the AI Risk Management Framework (RMF), likewise a soft-law instrument, intended for public and private organisations for identifying and mitigating the risks associated with AI systems²⁴.

In the absence of a general federal law, regulation takes place at state level:

The Illinois Biometric Information Privacy Act (BIPA, 2008) imposes the obligation of written consent for the collection of biometric data and regulates the possibility of an action for damages²⁵.

The California Consumer Privacy Act (CCPA, 2018), as amended by the California Privacy Rights Act (CPRA, 2020), regulates the collection of personal data and introduces special rights with respect to the use of automated decision-making technologies: the right of access regarding the use of automated decision-making technology; the right to object to the use of automated decision-making technology; and, where appropriate, the right to request human review of the automated decision²⁶.

This decentralised approach has the advantage of encouraging innovation and the experimentation of legislative solutions, so that practice may show which regulatory model is better, thereby providing new (more solid) bases for future normative acts; its greatest disadvantage, however, is normative fragmentation and uncertainty (the rules and solutions differing from one American state to another).

Canada has not, up to this point, regulated AI technology by means of a normative act; however, regulatory instruments do exist, with different nature and legal force. It is noteworthy that a distinction is made between the public and the private sector.

Within the federal public administration, Canada has built a firm framework based on administrative policy instruments issued within the Treasury Board system (one of the departments of the Canadian government)²⁷. The most important act is the Directive on Automated Decision-Making, launched in 2019 and entering into force on 1 April 2020. Through this act, the general policy regarding the use of AI in the public administration is established, setting a series of standards such as transparency, fairness, accountability, and the guarantee of avenues for challenging decisions taken by artificial intelligence. In application of the directive, another act was developed – the Algorithmic

²³ White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (Washington, DC: The White House, 2022), <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.

²⁴ NIST AI 100-1, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, (Gaithersburg, MD: National Institute of Standards and Technology, 2023), <https://doi.org/10.6028/NIST.AI.100-1>.

²⁵ Illinois Compiled Statutes, *Biometric Information Privacy Act*, 740 ILCS 14/1 et seq. (2008), <https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57>

²⁶ *California Consumer Privacy Act of 2018*, Cal. Civ. Code § 1798.100 et seq. (2018), as amended by the California Privacy Rights Act of 2020, Proposition 24 (2020), https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&lawCode=CIV&part=4.&title=1.81.5.

²⁷ Treasury Board of Canada Secretariat, “About the Treasury Board,” Government of Canada, modified June 13, 2025, <https://www.canada.ca/en/treasury-board-secretariat/corporate/about-treasury-board.html>.

Impact Assessment, an instrument intended to assess the risks of the use of AI.

In the private sector, at this time there are only soft-law instruments, guidelines – the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems (2023) and the subsequent implementation guidelines developed by Innovation, Science and Economic Development.

At present, the Artificial Intelligence and Data Act (AIDA), included in Bill C-27, is under parliamentary debate; this is a draft federal normative act of regulation with general vocation, intended to cover in a comprehensive manner the main legal aspects of artificial intelligence²⁸. The bill provides for:

- the classification of AI systems according to the risk they present;
- strict obligations of risk assessment and audit for providers of high-risk systems;
- severe sanctions, including criminal fines, for the development of dangerous or harmful AI systems.

The People's Republic of China has chosen a form of regulation consistent with the architecture and philosophy of the national legal system, a regulation characterised by centralisation, imperative rules, and the subordination of AI development to the objectives of national security and social control. AI regulation is contained in administrative normative acts issued by the Cyberspace Administration of China (CAC) and other competent authorities. These provisions do not have the status of laws adopted by the National People's Congress, yet they are binding; thus, the obligations of digital service providers and the mechanisms of administrative control are established in detail²⁹.

The “Provisions on the Administration of Algorithmic Recommendations in Internet Information Services” (2021) impose on algorithm providers a series of obligations: the obligation to register the models used with the competent regulatory authority, to ensure transparency of the algorithms and of the criteria on the basis of which AI takes decisions, and to prevent the use of algorithms for the purpose of manipulating the behaviour of human users.

The “Provisions on the Administration of Deep Synthesis Internet Information Services” (2022) regulate the use of deepfake technologies. They establish the following important obligations: clear labelling of synthetically generated content, prohibition of abusive uses or uses that may endanger a series of protected values (national security, public order, or the rights of individuals).

The “Interim Measures for the Administration of Generative Artificial Intelligence Services” (2023) establish a licensing regime for providers of services

²⁸ Canada, Parliament, House of Commons, *Bill C-27: Digital Charter Implementation Act*, 2022, 1st sess., 44th Parl., first reading, June 16, 2022, pt. 3, “Artificial Intelligence and Data Act.”

²⁹ The Legislation Law of the People's Republic of China (15 March 2000, as amended on 15 March 2015) classifies normative acts into laws (adopted by the National People's Congress), administrative regulations (issued by the State Council), and departmental regulations (issued by ministries and central agencies, such as the Cyberspace Administration of China). Normative acts adopted by the CAC fall within this latter category; they are binding in nature, but subordinate to the law. See Shiling Xiao and Yang Lin, “Judicial Review of Administrative Rules in China: Incremental Expansion of Judicial Power,” *Journal of Comparative Law* 17, no. 2 (2022): 371–392, <https://ssrn.com/abstract=4296692>.

involving AI. Obligations are instituted regarding the verification of the quality and legality of training data, as well as mechanisms for filtering and moderating generated content before publication, in order to prevent the dissemination of illegal or harmful materials.

Japan has not to date adopted a normative act, preferring a governance framework based primarily on soft-law instruments. Mention may be made of the Governance Guidelines for Implementation of AI Principles of 2021 or the AI Guidelines for Business of 2024. These guidelines contain only guiding principles, and it is for the developers of AI technologies to adopt and implement them and, on a case-by-case basis, to formulate their own (internal) rules starting from them. The central value protected in these official guidelines is the human being. The Governance Guidelines for Implementation of AI Principles of 2021 set out seven principles that should guide any activity in the AI field: human-centricity, education and literacy, privacy protection, security, fair competition, fairness, accountability and transparency, and innovation. The 2024 guide (AI Guidelines for Business) starts from three fundamental values – dignity, diversity and inclusion, sustainability – which it then develops into a number of recommendations (similar to the principles contained in the 2021 guide). This orientation is integrated into the broader strategic project of Japanese society, known as Society 5.0³⁰.

South Korea. In the Republic of Korea, the regulation of artificial intelligence has evolved in several stages. We may speak of a search for and maturation of AI regulatory solutions; it began with guidelines, soft-law instruments, a national strategy was developed, self-governance recommendations were issued, and, finally, a special law was drafted.

The first stage comprised only soft-law instruments. At the end of 2020, the Ministry of Science, Information and Communication Technology launched the National AI Ethical Guidelines. The guide is built around three basic principles: human dignity, the public good of society, and the appropriateness of technology to its purpose, developed into ten key requirements (including the protection of human rights, privacy, non-discrimination, accountability, safety, and transparency).

In 2021, the MSIT announced the Strategy to realize trustworthy artificial intelligence. The document is based on three pillars (technology, system, ethics) and ten action plans.

In 2022, the AI Ethics Self-Checklist and the Guidelines for the Development of AI Ethics Education Content were published in draft form. In the following years, other instruments were also developed (Guidebook for Trustworthy AI and AI Ethics

³⁰ “In the 5th Science and Technology Basic Plan (Cabinet decision of 22 January 2016), the concept of Society 5.0 was proposed for the first time as ‘a human-centered society in which economic development and the resolution of social problems are compatible with each other through a highly integrated system combining cyberspace and physical space. In order to give concrete form to, and bring into reality, the concept of Society 5.0 presented in the 5th Science and Technology Basic Plan, the 6th Science, Technology and Innovation Basic Plan (Cabinet decision of 26 March 2021) describes Society 5.0 as ‘a sustainable society that is resilient in the face of threats and unforeseen and uncertain situations, that ensures people’s safety and security, and that enables each individual to achieve diverse forms of well-being.’” Cabinet Office, cited from the official webpage.

Impact Assessment). These instruments translate the general ethical principles (contained in the first guidelines and in the national strategy) into development rules and impact-assessment mechanisms, with AI developers being expected to apply them voluntarily and/or to adopt their own rules on their basis.

The decisive step was taken through the adoption by the National Assembly of Korea, on 26 December 2024, of the Basic Act on the Development of Artificial Intelligence and the Establishment of Foundation for Trustworthiness, promulgated on 21 January 2025 and entering into force on 22 January 2026. According to Article 1, the purpose of the law “is to protect the rights and interests of the people, as well as their dignity, to improve the quality of life of the people, and to strengthen national competitiveness, by prescribing the basic matters necessary for the sound development of artificial intelligence and for the establishment of a foundation for trustworthiness.” The law provides for the periodic elaboration of an AI Master Plan, the establishment of a National Artificial Intelligence Committee and of an Institute dedicated to the study of AI safety, and introduces obligations regarding transparency, safety, and operator responsibility, especially for generative AI and high-risk AI systems. Worth noting is the special regulation of certain acts of an administrative and criminal nature³¹.

5. Conclusions

Law is intended to regulate social relations and to protect social values. The historical evolution of human society inevitably entails the emergence of new realities, some of great importance, which calls for legislative intervention in order to adapt and update legal norms. Major economic or technological revolutions have inevitably been accompanied by transformations of the law. This happened, for example, with the appearance of printing or with the industrial revolution. Of a subtler nature, but with major impact, were the appearance and large-scale spread of the Internet (at the beginning of the 1990s), and today the rise of artificial intelligence.

The present study started from the following question: can the law learn from the experience of Internet regulation in order to respond more adequately to the challenges generated by artificial intelligence?

The reaction of the legislator is clearly more prompt and the regulatory solutions are more adequate (including from the perspective of future developments). The explanation lies, in our opinion, in the experience accumulated through the regulation of legal relations carried out in the virtual environment, which emerged with the Internet era.

The appearance of the Internet surprised the legislator only through its novelty; however, it represents merely a virtual environment parallel to physical reality, in which, by and large, the same social relations take place. The legislator merely adapted the old legal institutions (the juridical act, the signature, the formation of the agreement

³¹ Republic of Korea, *Framework Act on the Development of Artificial Intelligence and the Creation of a Foundation for Trust*, Act No. 20676, promulgated January 21, 2025, effective January 22, 2026, Korean Law Information Center, <https://www.law.go.kr/lsInfoP.do?urlMode=eng&lsInfoR&lsId=014820>.

of wills, etc.). The experience of the Internet shows that the law reacted in stages and post factum. There was a succession in the reaction of the world of law to the new realities: academic debates, soft-law instruments adopted by international organizations, international conventions, European Union directives, and special normative acts (positive law) within the national legal order. Over time, regulatory solutions, even at national level, reached a certain degree of harmonisation.

If, in the Internet era, the legislator merely had to adapt old legal institutions in order to make them compatible with the digital environment, the emergence of artificial intelligence challenges the very nature of these institutions, so that we can no longer speak merely of adaptation, but of transformation. The legislator is compelled to rethink the very nature of certain classical legal categories, such as will, the juridical act, fault, or liability.

As in the case of the Internet, the first steps were taken through recommendations or guidelines adopted by international organizations, such as, for example, the Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021).

At national level as well, the process began with soft-law instruments, and only later did some states move to regulation through normative acts of positive law.

In synthesis, we may say that states have adopted several regulatory solutions, which may be grouped as follows:

a) regulation solely through soft-law instruments, usually called guidelines, drawn up by the competent ministries (research, technology and communications), together with research institutes or governmental agencies. In this way an horizon of expectations is created, all those involved in the development and exploitation of AI technologies being expected to observe these orientations voluntarily and, possibly, on their basis, to draft their own internal regulations. This is the case of Japan;

b) regulation through the adoption of normative acts of positive law, as the European Union did through the adoption of Regulation (EU) 2024/1689 (“AI Act”). EU regulations are directly applicable in all Member States;

c) in certain federal states, a decentralised and mixed model, in which the absence of a general federal law is compensated by soft-law instruments at central level and by sectoral or subnational normative interventions (the United States of America);

d) the dual model, in which the public administration is already subject to a binding administrative framework, while the private sector remains, for the time being, within the sphere of guidelines and voluntary codes (Canada);

e) the gradual model, in which soft-law instruments prepare the ground for subsequent legislative regulation (South Korea).

In Japan and South Korea, certain particularities may be identified. The soft-law instruments have a significant ethical and social-philosophical component; together they form a framework organised in layers, starting from fundamental values (which place the human being and social harmony at the centre) down to concrete implementation measures. In South Korea, a later stage brought regulation through normative acts of positive law (adopted through parliamentary procedure), whereas Japan, for the time being, has remained only at the first stage.

f) the administrative-centralised and imperative model, in which regulation is carried out through binding administrative acts, closely linked to security, control, and public order – China. Given the specific features of the organisation of the state and of political doctrine, China has preferred regulation through binding administrative acts that prioritise the idea of state control over artificial intelligence.

A common feature of the two periods (the Internet era and the artificial intelligence era) is that the first reaction was the adoption, by international organizations, of soft-law instruments, which prepared the ground for positive-law legislation.

We may say that, whereas the regulations that followed the emergence of the Internet were rather reactive, post factum, those regarding artificial intelligence have come more rapidly and are rather anticipatory in character, being oriented towards the rapid evolution of artificial intelligence in the future.

Bibliography

1. Abbate, Janet. *Inventing the Internet*. Cambridge, MA: MIT Press, 1999.
2. Berners-Lee, Tim, with Mark Fischetti. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. San Francisco: HarperSanFrancisco, 1999.
3. *Biometric Information Privacy Act*. 740 ILCS 14/1 et seq. (2008). <https://www.ilga.gov/Legislation/ILCS/Articles?ActID=3004&ChapterID=57>.
4. *California Consumer Privacy Act of 2018*. Cal. Civ. Code § 1798.100 et seq. (2018), as amended by the California Privacy Rights Act of 2020, Proposition 24 (2020). https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=3.&lawCode=CIV&part=4.&title=1.81.5.
5. Calo, Ryan. "Artificial Intelligence Policy: A Primer and Roadmap." *UC Davis Law Review* 51, no. 2 (2017): 399–435. <https://lawreview.law.ucdavis.edu/archives/51/2/artificial-intelligence-policy-primer-and-roadmap>.
6. Canada, Parliament, House of Commons. *Bill C-27: Digital Charter Implementation Act, 2022*. 1st sess., 44th Parl. First reading, June 16, 2022. Part 3, "Artificial Intelligence and Data Act." <https://www.parl.ca/legisinfo/en/bill/44-1/c-27>.
7. Căzănel, Maria, and Sorin Calafus. "The Notions of Parties, Third Parties and Successors in Title in Contractual Relations." In *5th International Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM 2018*, vol. 18, book 1.6, 299–304. 2018. <https://doi.org/10.5593/sgemsocialF2018/1.6/S02.037>.
8. Cerf, Vinton G., and Robert E. Kahn. "A Protocol for Packet Network Intercommunication." *IEEE Transactions on Communications* 22, no. 5 (1974): 637–648. <https://doi.org/10.1109/TCOM.1974.1092259>.
9. Directive 97/7/EC of the European Parliament and of the Council of May 20, 1997, on the protection of consumers in respect of distance contracts. *Official Journal of the European Communities* L 144 (June 4, 1997): 19–27. <https://eur-lex.europa.eu/eli/dir/1997/7/oj>.
10. Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999, on a Community framework for electronic signatures. *Official Journal of the European Communities* L 13 (January 19, 2000): 12–20. <https://eur-lex.europa.eu/eli/dir/1999/93/oj>.

11. Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). *Official Journal of the European Communities* L 178 (July 17, 2000): 1–16. <https://eur-lex.europa.eu/eli/dir/2000/31/oj>.
12. Directive (EU) 2024/2853 of the European Parliament and of the Council of October 23, 2024, on liability for defective products and repealing Council Directive 85/374/EEC. *Official Journal of the European Union* L 2024/2853 (November 18, 2024). <https://eur-lex.europa.eu/eli/dir/2024/2853/oj>.
13. European Commission. *Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)*. COM(2022) 496 final, 2022/0303(COD). Brussels, September 28, 2022. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496>.
14. High-Level Expert Group on Artificial Intelligence. *A Definition of AI: Main Capabilities and Scientific Disciplines*. Brussels: European Commission, 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341.
15. Law No. 365/2002 on electronic commerce. *Official Gazette of Romania*, Part I, No. 483, July 5, 2002.
16. Law No. 455/2001 on the electronic signature. *Official Gazette of Romania*, Part I, No. 429, July 31, 2001.
17. Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector. *Official Gazette of Romania*, Part I, No. 1101, November 25, 2004.
18. Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.
19. Mittelstadt, Brent, Chris Russell, and Sandra Wachter. “Explaining Explanations in AI.” In *Proceedings of the Conference on Fairness, Accountability, and Transparency*, 279–288. New York: Association for Computing Machinery, 2019. <https://doi.org/10.1145/3287560.3287574>.
20. OECD. *Recommendation of the Council on Artificial Intelligence*. OECD/LEGAL/0449. Adopted May 22, 2019. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.
21. Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act). *Official Journal of the European Union* L 2024/1689 (July 12, 2024). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.
22. Republic of Korea. *Framework Act on the Development of Artificial Intelligence and the Creation of a Foundation for Trust*. Act No. 20676. Promulgated January 21, 2025. Effective January 22, 2026. Korean Law Information Center. <https://www.law.go.kr/lsInfoP.do?urlMode=eng&lsInfoR&lsId=014820>.
23. Șandru, Daniel-Mihail. “Prolegomena on the Right to the Internet.” *Law Review* 15, no. 1 (2025): 32–41. <https://internationallawreview.universuljuridic.ro/index.php/journal/article/view/443>.
24. Tabassi, Elham. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology, 2023. <https://doi.org/10.6028/NIST.AI.100-1>.

25. Trandafirescu, Bogdan Cristian. *Teoria generală a dreptului. Curs universitar* [General Theory of Law: University Course]. Bucharest: Universul Juridic, 2025.
26. Treasury Board of Canada Secretariat. "About the Treasury Board." Government of Canada. Modified June 13, 2025. <https://www.canada.ca/en/treasury-board-secretariat/corporate/about-treasury-board.html>.
27. UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. Adopted November 23, 2021. Paris: UNESCO, 2021. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.
28. White House Office of Science and Technology Policy. *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*. Washington, DC: The White House, 2022. <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.
29. Xiao, Shiling, and Yang Lin. "Judicial Review of Administrative Rules in China: Incremental Expansion of Judicial Power." *Journal of Comparative Law* 17, no. 2 (2022): 371–392. <https://ssrn.com/abstract=4296692>.