The Regulation of Emerging Technologies in Greek Law

by **Antonios Broumas and Paola Charalampous** *

Abstract: The statue 4961/2022 in Greek Law sets out the national framework for the regulation of emerging technologies under conditions of trustworthiness, safety and cybersecurity, consumer protection, respect for fundamental rights and the democratic rule of law.

Part A' of the Law (articles 1-27) aims to establish an adequate institutional framework for the accomodation of the potential of AI by public and private sector bodies under conditions of fairness and security, as well as to strengthen the resilience of the public administration against cyber threats. In the context of serving this purpose, Part A of the Law includes regulations for (a) the development of artificial intelligence, and (b) upgradinginformation security and data protection in the public sector.

Part B of the Law (articles 28-57) aims at the exploitation by the public sector and the private market of the potential unleashed by advanced technologies and the maintenance of good practices, with the ultimate goal of consolidating the digital transformation of the country. For this purpose, Part B of the Law includes regulations regarding (i) the Internet of Things ("IoT"), (ii) Unmanned Aircraft Systems ("UAS"), (iii) distributed ledger, and (iv) 3D printing.

Keywords: Regulation, Emerging Technologies, Greece

Recommended citation: Antonios Broumas and Paola Charalampous, The Regulation of Emerging Technologies in Greek Law, 14 (2023) JIPITEC 594 para 1.

A. Introduction

1 The digital transformation of societies offers both challenges and opportunities, which are relevant to law. Regulatory interventions in relation to technology are mainly triggered by market failures, regulatory gaps, equity / fairness purposes and long-term public policy goals[1].

2 Along these lines, the European Union (EU) has taken a principled prescriptive approach for the regulation of technology, committed to putting people at the centre of the digital transformation, supporting solidarity and inclusion, promoting freedom of choice in a fair digital environment, fostering participation in the digital public space, increasing safety, security and empowerment, ensuring privacy and individual control over data and promoting sustainability[2]. To this end, the Digital Decade Policy Programme 2030 of the European Commission sets out the general objective on a Union level of

* Antonios Broumas is Attorney at Law, Digital Law Lead, EY Law Greece.

Paola Charalampous is Attorney at law, Compliance officer.

1 Jacques Pelkmans; Andrea Renda (2014). How Can EU Legislation Enable and/or Disable Innovation, p. 11.

2 European Declaration on Digital Rights and Principles for the Digital Decade, 2023/C 23/01, 23.1.2023, available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32023C0123(01).

the promotion of a human-centred, fundamental-rights-based, inclusive, transparent and open digital environment where secure and interoperable digital technologies and services observe and enhance Union principles, rights and values and are accessible to all, everywhere in the Union[3].

3 The digital transformation policy of the Greek state is mainly determined by the 2020-2025 Digital Transformation Bible issued by the Ministry of Digital Governance in June 2021[4]. The Bible sets out general principles for national policy making, which have also been adopted at statutory level by virtue of article 3 of the Framework Law 4727/2020 on digital governance[5]. Even though these principles primarily refer to the deployment of technology in the public sector, the Bible also provides for principles relevant for regulatory interventions in respect of emerging technologies, such as the principles of equality, trustworthiness and trust, openness and transparency, integrity, security and confidentiality.

4 In this context, on 27 July 2022, the Greek Law 4961/2022 "on emerging information and communication technologies, the reinforcing of digital governance and other provisions" was published and set in force[6], except for the provisions regarding artificial intelligence, which entered into force on 1 January 2023, and the provisions regarding Internet of Things devices, which entered into force on 1.3.2023.

5 The new Law sets out the national framework for the regulation of artificial intelligence ("AI"), the Internet of Things (IoT), the provision of postal services using Unmanned Aircraft Systems ("UAS"), the use of distributed ledger technologies ("DLT") and the conclusion of smart contracts, as well as the protection of works of three-dimensional printing ("3D Printing").

3 European Commission (2022). Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, OJ L 323, 19.12.2022, p. 4–26, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022D2481.

4 Greek Ministry of Digital Governance (2021). 2020-2025 Digital Transformation Bible, available: https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digital_strategy.pdf.

5 Greek Government Gazzette 184/A/23-09-2020, available: https://www.et.gr/api/DownloadFeksApi/?fek_pdf=20200100184.

6 Greek Government Gazzette 146/A/27-07-2022, available: https://www.et.gr/api/DownloadFeksApi/?fek_pdf=20220100146.

B. Background, Purpose & Scope

6 Law 4961/2022 regulates the utilization and use of a basic set of contemporary emerging technologies with significant economic and social impact. It thus lays down the conditions for the rapid adoption and development of these technologies in Greek economy and society, with the ultimate goal of promoting the country's digital transformation.

7 In terms of scope, the new Law enacts vertical obligations for providers of products and services related to AI, IoT and UAS in the transport industry, and horizontal requirements for the use of AI and 3D printing, while laying the foundations for conducting transactions with DLTs and smart contracts.

8 In this respect, the Law introduces prescriptive statutory interventions in areas which have been deemed by the Greek legislature as constituting regulatory gaps producing sub-optimal outcomes in relation to public policy objectives, such as the protection of end-users, the promotion of innovation and the resilience of key emerging technologies vis-à-vis cyber-risks.

9 The purpose of Law 4961/2022 is, on the one hand, the lawful, safe and secure development, deployment and use of AI technologies by public and private entities and, on the other hand, the accommodation of the potential of IoT, UAS, DLT and 3D Printing for the public sector and the market[7].

10 The provisions of Law 4961/2022 unfolds in four parts, which concern, among other things, the digital upgrade of public administration (Part A') and the utilization of emerging technologies by public bodies and private entities (Part B').

11 In specific, Part A' of the Law (articles 1-27) aims to establish the adequate institutional framework for the exploitation of the potential of AI by public and private sector bodies under conditions of fairness and security, as well as to strengthen the resilience of the public administration against cyber threats. In the context of serving this purpose, this part includes regulations for (a) the development of artificial intelligence, and (b) the upgrade of information security and data protection in the public sector.

12 Furthermore, Part B of the Law (articles 28-57) aims at the exploitation by the public sector and the private market of the potential unleashed by advanced technologies in line with good practices, with the ultimate goal of consolidating the digital transformation of the country. For this purpose, Part B of the Law includes regulations regarding (i) the Internet of Things ("IoT"), (ii) Unmanned Aircraft

7 See articles 1 and 30 of Law 4961/2022.

Systems ("UAS"), (iii) distributed ledger, and (iv) 3D printing.

C. The Greek Legal Framework for the Regulation of AI

13 The application of artificial intelligence ("AI") technologies is expected to transform the economy, work and society in general. Still, the provision, deployment and use of AI systems raises serious ethical issues[8], whereas it also poses risks for fundamental rights, the safety and security of persons and property and the democratic rule of law[9].

14 Taking into account the forthcoming adoption of the Artificial Intelligence ("AI") Act by the European Union ("EU")[10], the Greek Law 4961/2022 introduces supplemental national provisions for the regulation of AI use in the Greek public and private sectors. In respect of coherence, the Greek law does not generally overlap with the subject matter of the forthcoming AI Act, by regulating (i) the deployment of AI in the public sector; (ii) the use of AI in the private sector with specific requirements related to ethical use and the protection of employees.

15 The national framework follows a prescriptive "risk-based" approach for the regulation of AI in line with the proposed AI Act, enacting the following obligations per category of obligated entities:

I. AI in the Public Sector

16 Provision by Statute: Except for the Ministries of National Defense and Citizen Protection, the use of AI systems is permitted only by a special provision by statute, which includes appropriate safeguards for the protection of the rights of natural or legal persons affected by these systems[11].

17 Algorithmic Impact Assessment: Before deploying AI systems, in addition to performing a data protection impact assessment of Regulation (EU) 2016/679 ("GDPR"), public bodies shall have the obligation to execute algorithmic impact assessments in order to evaluate the risks that may arise to the rights, freedoms and legitimate interests of the persons affected by such AI systems[12]. Appropriate safeguards for the protection of the rights of persons affected by the use of AI systems shall be further specified through the issuance of a Presidential Decree[13].

18 Operational Transparency: Each public body shall publicly disclose information, inter alia, about the commencement of operation and the operating parameters of any AI systems deployed as well as on the decisions taken or supported through them. Any complaints by affected persons on violations of transparency obligations shall be examined by the National Transparency Authority[14].

19 Register of AI Systems: Each public body shall maintain a register of the AI systems it uses[15].

II. AI in the Private Sector

20 AI in the Employment Context: Prior to the deployment of an AI system, which affects the decision-making process concerning employees, existing or prospective, and has an impact on their conditions of employment, selection, recruitment or evaluation, private entities shall provide relevant information to the employee. This obligation also applies to digital platforms in respect of natural persons linked to them by employment or independent service contracts or project agreements. For any violation of this obligation, the Labor Inspectorate may impose monetary sanctions[16].

8 European Commission High-Level Expert Group on AI ("AI HLEG"), Ethics Guidelines for Trustworthy Artificial Intelligence, 8 April 2019, available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

9 OECD Working Party and Network of Experts on AI, Advancing accountability in AI, Governing and managing risks throughout the lifecycle for trustworthy AI, February 2023, No. 349, available: https://www.oecd-ilibrary.org/deliver/2448f04b-en.pdf?itemId=%2Fcontent%2Fpaper%2F2448f04b-en&mimeType=pdf.

10 European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act), COM/2021/206 final, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

11 See article 4 of Law 4961/2022.

12 The institution of the algorithmic impact assessment of the Greek Law 4961/2022 draws elements from the corresponding institutions established in the Canadian Directive on Automated Decision Making and the US 2022 Algorithmic Accountability Act (H.R. 6580).

13 See article 5 of Law 4961/2022.

14 See article 6 of Law 4961/2022.

15 See article 8 of Law 4961/2022.

16 See article 9 of Law 4961/2022.

21 Ethical Use of Data: Any medium- or large-sized undertakings within the meaning of article 2 of Law 4308/2014[17], shall be obliged to adopt a policy for the ethical use of data, which includes information on the measures, actions, and procedures they apply to data ethical issues when using AI systems. In addition, entities obliged to issue corporate governance statements in accordance with article 152 of Law 4548/2018, must include in it information about their data ethics policy. The content of such policies shall be further specified through the issuance of a Joint Ministerial Decision[18].

22 Record of AI Systems: Any medium- or large-sized undertakings within the meaning of article 2 of Law 4308/2014 shall maintain a record of the AI systems deployed[19].

III. AI & Public Procurement

23 Finally, the new Law establishes the following national requirements for public procurement procedures for the design or development of AI system[20]:

24 i. The contractor shall furnish the contracting authority with information necessary to fulfil its transparency requirements on AI system operation stipulated in the Law;

25 ii. The AI system shall be delivered in such a way so that the contracting authority be able to study its mode and parameters of operation, to further improve it and to publish or make available, in any way, those improvements; and

26 iii. Appropriate measures will need to be taken to bring the AI system in line with applicable laws, in particular, regarding the protection of human dignity, the respect for private life and the protection of personal data, non-discrimination, equality between women and men, freedom of expression, universal access for persons with disabilities, workers' rights, and the principle of good administration.

27 It is explicitly stipulated that the provisions of Law 4961/2022 on AI technologies do not affect the rights and obligations provided for in the GDPR and supplementary Law 4624/2019 on the protection of personal data.

28 Finally, the new Law establishes, on the one hand, a Coordinating Committee for AI with responsibilities for the drafting of the National Strategy for AI and, generally, the formulation of policy around AI and, on the other hand, a Committee for the supervision of the strategy, which ensures the implementation, the coordination of the competent bodies and manages its enforcement.

29 To carry out their work, the two committees receive data and know-how from the national AI Observatory, also established by the Law, which has the duty to monitor and report on technological developments and policies around AI in the country and at an international level.

D. Provisions on Information Security & Data Protection

30 Law 4961/2022 further establishes the following institutions for shielding the country against threats related to information and network security[21]:

31 The General Directorate of Cybersecurity of the Ministry of Digital Governance is designated as the National Cybersecurity Certification Authority in accordance with article 58 of Regulation (EU) 2019/881. Ministerial decisions shall define the monitoring procedure and the bodies assessing the products, services and ICT procedures vis-a-vis the requirements of European cybersecurity certificates, as well as the relevant sanctions in case of non-compliance.

32 The Ministry of Digital Governance establishes the Hybrid Threat Analysis Observatory, i.e. the advisory body of the National Cybersecurity Authority with responsibility related to the analysis and prevention of hybrid threats in the field of cybersecurity.

33 The General Directorate of Cybersecurity of the General Secretariat for Telecommunications and Post of the Ministry of Digital Governance is designated as the national coordination center as per Article 6 of Regulation (EU) 2021/887.

34 In each central government body, an Information and Communication Systems Security Officer ("ICSSO") is

17 According to the respective provisions of Law 4308/2014, medium-sized undertakings are those which fulfill two or more of the following criteria: (i) 250 employees, (ii) a turnover of up to €40 million and (iii) a net balance sheet total of up to €20 million. For large-sized undertakings the respective criteria increase up to: : (i) 250 employees, (ii) a turnover of up to €40 million and (iii) a net balance sheet total of up to €20 million

18 See article 10 of Law 4961/2022.

19 See article 10 of Law 4961/2022.

20 See article 7 of Law 4961/2022.

21 See articles 3-26 of Law 4961/2022.

appointed, with the task of supervising the security of the entity's network and information systems and ensuring the issuance of a risk analysis plan and the security policy of the Body's ICT systems.

35 Each public body having a critical infrastructure also designates a Security Coordinator, who carries the duties of the ICSSO for this particular infrastructure.

36 Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) created a European Union-wide cybersecurity certification scheme in the field of information and communication technology and strengthened ENISA by defining its specific role and responsibilities. The General Data Protection Regulation focuses on "Data Protection by Design", where components related to both privacy and security meet, whereas the European Regulation on Cybersecurity focuses on "Security by Design", which enables the products' designers and constructors to receive the relevant certification and consequently strengthens the public confidence in the above products and services[22].

37 As per the new Law, providers of public electronic communication networks are required to have in place and align with an information security risk assessment plan, which they shall update on an annual basis. Also, a procurement plan in relation to the equipment obtained and the participation of third-party suppliers.

38 Finally, a register of data protection officers of public sector bodies is established as well as a relevant committee for the exchange of expertise and cooperation with ISDPS.

E. The Greek Legal Framework for the Regulation of IoT

39 According to the European Commission, "machine-generated data is created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real"[23].

40 Machine-generated data can be both personal or non-personal in nature. Machine-generated data that may result in the identification of an individual qualify as personal data, as in the case of data generated by wearable devices[24].

41 Law 4961/2022 sets out a comprehensive framework of national rules for the cybersecurity of Internet of Things ("IoT") devices through the enactment of primary statutory provisions and secondary administrative rules. The Law also establishes the National Cybersecurity Authority as the authority competent for the supervision and implementation of its rules.

42 According to the definitions of Law 4961/2022, IoT means any technology that[25]:

(a) allows devices or a group of interconnected or related devices, through their internet connection, to perform automatic processing of digital data; and

(b) enables the collection and exchange of digital data, in order to offer a variety of services to users, with or without human participation.

43 Law 4961/2022 imposes legal obligations on both manufacturers and importers / distributors and, also, operators of IoT devices[26].

44 According to the provisions of the new Law, manufacturers are required to accompany IoT devices with a declaration of compliance with the technical safety specifications, indicated in the law, as well as instructions for use and information on safe use.

45 In addition, each manufacturer is obliged to have a management process in place in relation to its IoT devices, in cases where it is ascertained by the user that: a) a security incident occurs, or b) a vulnerability exists in the security parameters of the device. This process should include appropriate documentation by the manufacturer about the nature and possible forms of occurrence of the security incident or the vulnerability, detailed instructions for dealing with them, as well as indicative measures to mitigate potential adverse consequences.

46 Importers and distributors are required to verify that the IoT devices they import or distribute are accompanied by a relevant declaration of compliance, as stipulated in the new Law, refrain from further import or distribution in case of absence and cooperate with competent public authorities for

22 A. Michailaki, Law and Ethics in the applications of augmented reality, Nomiki Vivliothiki, 2022, p. 24-25.

23 European Commission, Communication on "Building a European Data Economy, COM/2017/09 final, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN.

24 I. Igglezakis, "The Law of the Digital Economy", 2022, Sakkoula Publications, p. 52.

25 See article 31 of Law 4961/2022.

26 See articles 32-35 of Law 4961/2022.

matters of compliance with the provisions of the Law.

47 On the other hand, operators of IoT devices are obliged to follow the technical safety specifications of the devices they deploy and use. They should also appoint an IoT Security Officer to monitor the security measures of their devices. Furthermore, they are required to maintain a register of IoT devices, updated on an annual basis and, each time they put into service a new IoT device. Finally, each IoT operator should carry out an impact assessment of the planned personal data processing operations related to the operation of the IoT technology device.

48 The National Cybersecurity Authority is appointed as the competent authority to oversee the implementation of the national IoT security framework[27]. The Authority has the power to:

49 Require from manufacturers, importers, or distributors of IoT devices to take all necessary corrective actions in order to comply with the applicable legislation.

50 Order the temporary withdrawal from the market of IoT appliances presenting risks and their replacement in the market only if such risks have been removed.

51 Upon the Authority's recommendation, the competent body of the Ministry of Digital Governance may impose penalties of up to € 15,000 and, in case of relapse, of up to € 100,000 on non-compliant manufacturers, importers, distributors and operators.

52 Forthcoming ministerial decisions shall specify the technical specifications and safety measures of IoT devices, the obligations of manufacturers, importers, and suppliers of such products as well as the relevant sanctions in case of non-compliance.

53 It should be stressed that, to the extent that generated data constitutes personal data, providers and operators of IoT devices shall also be obliged to ensure a level of security appropriate to the risk by implementing appropriate technical and organizational security measures in line with article 32 of the GDPR[28]. Furthermore, should generated data also constitute communications and related traffic data, providers and operators of IoT devices shall be obliged to comply with the provisions of article 4 of Law 3471/2006 on the confidentiality of communications, transposing Directive 2002/58/EC into Greek law.

F. Provisions on the Use of UAS in the Context of Postal Services

54 With the aim of promoting innovation through the emerging technology of UAS in the postal sector, the new Law 4961/2022 lays down a set of rules facilitating the adoption of UAS technologies by postal service providers in conditions of legal certainty and clarity.

55 In specific, articles 43-46 of Law 4961/2022 amend the respective provisions of Greek Framework Law 4053/2012 on Postal Services[29], by introducing rules on the use of Unmanned Aircraft Systems ("UAS") in the postal sector.

56 The new Law explicitly stipulates that the provision of postal services, for which a general or special permit has been granted, in all or part of the Greek territory, may be carried out using UAS, subject to approval by the National Telecommunications and Post Commission ("NTPC")[30].

57 The use of frequencies by UAS for the provision of postal services shall be governed by the Delegated Regulation (EU) 2019/945 and the Implementing Regulation (EU) 2021/664[31].

58 According to the new Law, the technical characteristics and safety specifications of UAS used for the provision of postal services, as well as any other relevant issue, shall be specified through a decision issued by the Minister of Digital Governance, following an opinion of the NTPC and the Civil Aviation Authority[32].

27 The General Directorate of Cyber Security, part of the General Secretariat of Telecommunications & Posts of the Ministry of Digital Governance, has been designated as the National Cybersecurity Authority of Greece. The official website of the Authority is available here: https://mindigital.gr/dioikisi/kyvernoasfaleia.

28 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

29 Greek Government Gazzette 44/A/07-03-2012, available: https://www.et.gr/api/DownloadFeksApi/?fek_pdf=20120100044.

30 See article 45 of Law 4961/2022.

31 See article 46 of Law 4961/2022.

32 See article 45 of Law 4961/2022.

G. The Greek Legal Framework for the Regulation of DLT & Smart Contracts

59 At EU level, distributed ledger technologies ("DLTs") are already regulated by the MiCA[33] and DLT[34] Regulations. The national provisions of Law 4961/2022 complement these Regulations, by only regulating the applications of DLTs in smart contracts. In particular, the new Law 4961/2022 incorporates general rules for the validity and force of proof of smart contracts in a future-proof manner in order to promote the deployment and use of respective general-purpose technological solutions in the country.

60 Statue 4961/2022 defines "distributed ledger" as the repository of information that maintains records of transactions, and which is shared and synchronized between a set of DLT network nodes, using a consensus mechanism[35].

61 Furthermore, a blockchain is defined as a special type of distributed ledger technology that records data in blocks, which are connected to each other in chronological order and form a chain of a consensual, decentralized and mathematically verifiable nature, which is mainly based on the science of cryptography[36].

62 The foregoing definitions are fully aligned with the respective definitions of DLT and in article 3 of the MiCA and article 2 of the DLT Regulations.

63 Statue 4961/2022 goes forward to define a smart contract as a set of coded computer functions, which is finalized and executed through distributed ledger technology in automated electronic form through instructions for the execution of actions, omissions, or tolerances, which are based on the existence or not of specific conditions, according to terms recorded directly in electronic code, scheduled commands, or programmed language[37].

64 In smart contracts, trust in the person of the counterparty is replaced by trust in the very system of blockchain technology to which they belong. Because of the technical guarantees it provides, that system is presumed not to make any errors. The nature and role of participants in the DLT ecosystem determines their legal liability for any damage caused by their acts or omissions[38].

65 The new law lays down the foundations for the validity of smart contracts executed within the jurisdiction of Greece. According to its provisions, the recording of data or the execution of contracts may be freely conducted through a blockchain or other DLT, rendering valid the declarations of will exercised in such a form[39]. Smart contracts bind contracting parties as per the general provisions of the Greek Civil, including its provisions on invalidity of private contracts or declarations of will[40].

66 The provisions of Law 4961/2022 also stipulate that the submission of information or data about smart contracts executed through blockchain or other DLT fulfills the legal concept of private document[41] and suffices as valid proof for their execution before national courts. An official expert report may also be submitted for the verification of the transposition of the respective software code into text[42].

33 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114.

34 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0858.

35 See article 31 of Law 4961/2022.

36 See article 31 of Law 4961/2022.

37 See article 31 of Law 4961/2022.

38 L. Kanellos, 'Smart Contracts: Legal challenges and business prospects', Nomiki Vivliothiki, 2021, p. 163.

39 See article 47 of Law 4961/2022.

40 See articles 130, 138, 159, 174-179 and 140-157 respectively of the Greek Civil Code.

41 According to article 445 of the Greek Code of Civil Procedure, private documents, drawn up in accordance with the law, if their authenticity has been recognized or proved, constitute valid evidence that the statement they contain originates from the issuer of the document, but counter-evidence is permissible. Under the same conditions, private documents constitute valid evidence as to the content of declarations of will.

42 See article 51 of Law 4961/2022.

H. The Greek Legal Framework for the Regulation of 3D Printing

67 The Greek framework Law 2121/1993 on copyright does not include specific provisions for the regulation of authors' rights in relation to 3D printing designs and works. In this context, the Greek legislature has prioritized the adequate protection of intellectual property rights in this area as means to promote the unencumbered production, distribution and consumption of respective works of authorship. To this end, articles 53-57 of Law 4961/2022 set out the national framework for the regulation of the copyright law implications of 3D printing.

68 3D printing may be defined as the additive manufacturing technique by which, through successive deposition of successive layers of material, three-dimensional objects are made. This method has wide use in the production of spare parts and application in architecture, medical technology, weapons industry, industrial technology, etc[43].

69 In the new Law, "3D Printing" is defined as the process of uniting 3D printing materials through the technique of prosthetic successive stratification of such materials by using new technologies, especially 3D printers, and aiming on printing a physical object based on a digital model[44].

70 The new Law introduces the following amendments to Greek Framework Law 2121/1993 on copyright regarding works of speech on 3D printing[45]:

71 Any Computer Aided Design File (C.A.D. File) is explicitly characterized as a protected work of speech, as long as it includes a source code.

72 3D printers are expressly subject to a 4% private levy on their value for the benefit of authors and right-holders of neighboring rights.

73 Moreover, the new Law prohibits the use, sharing and hosting on online platforms of digital models or digital design files with the help of a computer or digital files of a typical triangle language or digital model design databases, without the prior permission of their right-holder[46].

74 As an exception, such acts are lawfully conducted without the permission of their right-holder if they are carried out solely for: (a) private, judicial or administrative use; (b) use for the benefit of persons with disabilities; (c) use for temporary or ancillary phases of a technological process that do not have independent economic significance; d) the fulfillment of educational or research purposes; (e) news purposes; or (f) the use of images or objects in public places or exhibitions in museums or in exhibits catalogues, provided that, in the above cases, the normal utilization of the work or other protected subject-matter is not affected and the legitimate interests of the author or the rightful owner are not unduly prejudiced.

75 The new Law also provides for the liability of online platform providers, through which digital models or digital files, without source code related to the 3D printing process, are used, shared, or hosted, in cases that, after becoming aware of the infringement, they do not take all necessary measures to remedy it[47].

76 Finally, the new Law establishes the liability of the creator or legal owner or seller, as the case may be, towards consumers for defective digital models or files related to the 3D printing process or three-dimensional printed objects or three-dimensional printers or scanners.

I. Critical Evaluation of the Greek Legislation on Emerging Technologies

77 According to well-established practices, the regulation of technology ought to be comprehensive, coherent, proportionate, evidence based, fit for purpose, future-proof and open to innovative solutions in a context of ever more rapid technological, societal and environmental change[48].

78 The subject-matter of the Greek Law 4961/2022 is focused on specific technologies, which have been held as "emerging" technologies of significant economic potential and social impact. The two-fold purpose of the Law is the constitution of an institutional environment appropriate, on the one hand, for the diffusion of the use of such technologies in Greek society, to accommodate innovation and facilitate digital transformation, and, on the other

43 M. Milapidou, 'New Technologies in Health: Medical, Legal and Ethical Issues', Nomiki Vivliothiki, 2021, p. 94.

44 See article 31 of Law 4961/2022.

45 See article 53 of Law 4961/2022.

46 See article 54 of Law 4961/2022.

47 See article 55 of Law 4961/2022.

48 European Commission Staff Working Document (2021). Better Regulation Guidelines, Brussels, 3.11.2021, SWD(2021) 305 final, p. 8, available: https://commission.europa.eu/document/download/d0bbd77f-bee5-4ee5-b5c4-6110c7605476_en?filename=swd2021_305_en.pdf.

hand, the pre-emption of possible harms or sub-optimal outcomes arising from these technologies (e.g. cyber-threats). In respect of AI regulation, the Law also employs a proportionate approach, imposing obligations only to medium- or large-sized undertakings. Furthermore, the Law establishes a robust institutional framework for the supervision of most of its requirements related to cybersecurity and AI.

79 Taking into account its Explanatory Statement, the Greek Law on emerging technologies appears to employ a patchy, rather than systematic, approach for the regulation of emerging technologies, by addressing certain regulatory gaps in the Greek legal order in relation to specific technologies. Furthermore, the choice of these technologies as the subject matter of regulation or the identification of respective gaps does not seem to arise on the basis of an evidence-based approach, thus running the risk of missing technologies or gaps that also require regulation due to their potential or impact. Furthermore, the Law is not the solid outcome of a comprehensive national innovation strategy and, therefore, falls short of a systematic and holistic approach to accommodate the potential of emerging technologies and effectively boost the digital transformation of the public and private sectors. Finally, the possible overlaps of the provisions of the Law with already adopted or forthcoming EU legislation, especially the AI Act, the Data Governance Act[49] and the NIS 2 Directive[50], may result in lack of regulatory coherence or over-regulation.

80 Overall, Law 4961/2022 constitutes a distinct national approach to the regulation of emerging technologies in the member-states of the European Union, with innovative national provisions that may be appropriate for other national jurisdictions.

J. Conclusion

81 Artificial intelligence is a rapidly evolving technological field that is expected to radically transform major aspects of Greek society, such as the economy, health, as well as entrepreneurship and innovation. In addition, the Internet of Things is at the core of the fourth industrial revolution, offering solutions in many areas of economic and social life, such as extremely fast response services, reliable remote solutions, using applications with greater ease, decision support, better resource allocation and remote control of services. Furthermore, the use of Unmanned Aircraft Systems in postal services presents advantages in terms of environmental protection (smaller environmental footprint) and access to critical or island areas, as well as areas with difficult access. Accordingly, the lack of regulation in respect of distributed ledger technologies results in legal uncertainty for innovative businesses and acts as disincentive for attracting investment, while at the same time the potential of these technologies remains untapped. Finally, the diffusion of 3D Printing technologies across business sectors requires the protection of respective intellectual property rights[51].

82 The provisions of Law 4961/2022 establish a national regulatory framework aspiring to promote these emerging technologies in Greece under conditions of trustworthiness, safety and cybersecurity, end-user protection, respect for fundamental rights and the democratic rule of law. Yet, the Law falls short of constituting a comprehensive national approach to the regulation of innovation. It therefore, remains to be seen whether the provisions of the new Law will contribute to technological innovation and result in a positive impact on the overall digital transformation of the public and private sectors of the country.

49 European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

50 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, available: https://eur-lex.europa.eu/eli/dir/2022/2555.

51 See Explanatory Statement to Law 4961/2022.