# THE INTERACTION OF EMERGING TECHNOLOGIES WITH THE LEGAL FIELD

## S. TOPOR

**Sorin TOPOR**
National Institute for Research and Development in Informatics - ICI Bucharest
E-mail: sorin.topor@ici.ro
ORCID ID: https://orcid.org/0000-0001-6212-3223

*Abstract*

*Artificial intelligence (AI) is currently perceived as the most disruptive emerging technology, with more and more members of contemporary society seeing it as a significant driver of job loss. Without understanding the opportunities to transform labor relations through the emergence of new professions and the abandonment of those professions that can be replaced by automation, technologies based on artificial intelligence are considered a formidable adversary of humanity and not a tool created to production processes support. On the other hand, more and more companies are implementing emerging technologies to automate production processes, to optimize management, to implement effective security solutions and to diversify communication.*

*In this context, we aim to analyse how and in what way emerging technologies will interact with the legal field and propose a picture of future work reports. It is becoming increasingly clear that social resilience also requires an adequate legal framework, able to adapt to the new challenges caused by the digitization of the labor market.*

*The National Institute for Research and Development in Informatics - ICI Bucharest is concerned with scientific research and applied development, actively involved in ensuring the cyber security of the identity of any person, natural and legal, and through the solutions for the sustainability of the digitalized society, it supports the national effort to ensuring cyber security, an important part of national security.*

*Keywords: emerging technologies, artificial intelligence, law, digital sustainability.*

## INTRODUCTION

Today, more and more companies are implementing emerging technologies especially for automating governance processes and optimizing product delivery. These solutions are extremely effective for increasing productivity, but they produce social convulsions in terms of the increased demand for new professions and qualifications that presuppose a rapid reconversion of the labor force.

Such a change also requires an adaptation of the legal framework to regulate the new labor relations. In this way, innovations that stimulate differentiation and competitive efficiency are highlighted, behaviours are modeled, but new approaches are also required regarding the dimension of the security of the identity of individuals in the general context of maintaining the security of the democratic state.

## I. GENERAL LEGAL CONTEXT APPLICABLE TO THE DIGITAL ECOSYSTEM

The modern state represents a construction whose formation and organization is based on society. The background of its dynamics is the legal framework made up of all social norms and rules (*Mihăilescu, S. L. Th., 2023, p.17*). Therefore, the law organizes life in common representing the technique of human coexistence intended to form a discipline that defends society from excesses. Within a society based on law, social relations are formed through legal rights and obligations, the observance of which is ensured, if necessary, by the coercive force of the state.

The information society represents the structuring of human society through the prism of information systems. By deduction, the digitized society represents an approach to the state through the digitization of digital resource relations. Digitization represents the process of transforming information into elementary units, measurable in bits, through which, with the help of specific technologies, objects, images, sounds or signals can be created. This transformation involves procedures that characterize the totality of interactions and relationships between people, processes, data and equipment in an organization involved in its information, decision-making, production and business processes.

The dimension of security is included in the information dimension, being determined by the value of knowledge in the field of interest. In the context of digitization, this must be "cyber" and characterizes the relationships of critical infrastructures, in particular, informational ones.

The presence of legal dimensions, in all information systems, makes sense as a support of the cyber dimension in the context of any approach to security (*Dinu, M.-Şt. 2022, pp.102-110*). In this way, solid legal instruments can be created that protect both individual rights and freedoms and ensure the protection of critical infrastructures of national or international interest. The coercive force

of the state and international organizations vis-à-vis non-state actors will apply to organized crime and terrorist structures, national, international and cross-border. Both organized crime and terrorism produce threats in the evolution of any information society, through cyber.

Therefore, if the regulatory object of civil law represents those social relations that are regulated by legal norms (*Boroi & Anghelescu, 2021, p.7*), we can affirm that the regulatory object of a new discipline, such as information law, can be represented by the correlation of all the regulations of informational law norms, during the procurement, storage and processing of information, regardless of the technology used. This will study the types of behaviour in digital relationships and will form a specific legal framework that includes norms and laws related to each element of the composition of information systems, components of the information ecosystem.

The function that enables the efficient evolution of the components of any information system is identity. Thus, system components can identify themselves and will gain authorized access for their participation in technological processes. Policies and procedures become the basic tools for preventing unauthorized access to various private data and information. Control of access to data and information is essential to block identity theft, violation of the right to privacy, violation of copyright and related rights, non-compliance with industrial property rights, violations of related rights legislation, intrusions into various components digitized for the purpose of hijacking critical information infrastructures necessary for the operation of critical sector components.

On the other hand, security and control policies and procedures must be carried out in accordance with legal provisions in the field of human rights, with regard to individual and civil rights and freedoms. They regulate the situations in which technical supervision, personal data protection, access to public information, etc. are required, and special attention must be given to them through constitutional norms and special laws. Thus, within the relations between the components of the information systems, new legal relations will not be generated that do not conform to social values.

We can affirm with real grounds that the historical stage we are going through represents a critical moment in the evolution of cyber-systems. Advances in computing, IT and communication systems have enabled the emergence of a wide range of digitized technologies, of which those based on artificial intelligence are becoming increasingly used. All this form the content of the concept of emerging technologies.

It is observed that, in some situations, the focus on the direction of technological developments has led to the emergence of an incoherence or a mismatch in cyber security.

It is known that the economic systems of a state are governed by functional requirements and markets in constant motion. Digital devices appear

and expand at an exponential rate, inversely proportional to the costs of their production. Their operational and finished product designs are evolving rapidly. New technological standards are emerging. Many devices that are already deployed have limited lifetimes, measured in years.

It is worth noting that these systems, whether they relate to a car's frontal collision prevention capability, a medical device's ability to adapt to circumstances in real time or the latest innovation in IoT, are a source that ensures the advantage competitive in the innovative economy (Industry 4.0), but generates various risks and vulnerabilities that can be exploited in hack activities (*Ciupercă, Cîrnu, Stanciu & Cristescu, 2022*).

The consequences of unintentional mistakes or malicious attacks can have a serious impact on the quality of human life and the environment. For this, every citizen, together with specialized structures, must make proactive efforts, coordinated through measures and procedures, to strengthen the cyber security culture and trust in emerging technologies. This is the only way to create legal norms correlated with the requirements of the digital environment, thus allowing the formation of a concrete and coherent cyber security policy (*Vevera, 2019, p.167*). In addition, cybersecurity must become a priority concern for everyone involved in the development of emerging technologies, from designers to administrators and users, as the digital ecosystem becomes part of our culture.

## II. LAW AND EMERGING TECHNOLOGIES

The current comfort of modern life is unthinkable without the use of emerging technologies. Digital information processing provides food supply, human mobility, health maintenance, entertainment and other social functions. Digitization is recognized as the main driver of economic relations. Within progressive views, economic freedom, deregulation and digital bans, etc. all support individual freedom. However, the omnipresence of digital media, without adequate legal regulations, can affect, first of all, the capacity for self-determination.

The adaptation of the labor force to the new requirements is also signaled in the Report "The Future of Jobs" (World Economic Forum, 2023), published on April 30, 2023, by the Global Economic Forum. The paper presents a reasoned perspective on how socio-economic and technological trends will shape the job market. Based on sociological research, it is estimated that a number of professions will disappear in the next five years and new professions will be created. Digital technology will change the way work is done, the job content and the skills needed by future workers. The entire industry will focus on big data analysis, cloud computing, computational functions and AI, environmental management, encryption technologies and cyber security. About 75% of the companies surveyed confirmed that they will adopt these technologies in the next five years. The data also shows the impact of digitization of commerce and

occupations, with digital platforms and applications. These technologies are likely to be adopted by 86% of industrial companies compared to 75% of e-commerce and digital commerce companies. On a lower place in the pace of implementation of emerging technologies are the entities in which there is a pronounced emphasis on the displacement of jobs, such as those in the field of agriculture, digital platforms and applications, those in electronic and digital commerce. They will use AI only in the situation where they want to achieve a professional compensation through reconversion. Their expectations for implementing AI to improve performance are to solve more than 50% of tasks through automation.

Professions related to electronics, chemistry and advanced materials industries are much more willing to adopt new technologies than those related to personal services, insurance and pensions. Those in management services and real estate are the least inclined to adopt emerging technologies.

We can appreciate that without a renewal of strategies and a reanalysis of priorities, many production structures will be left behind or disappear from the market, a situation that will produce social movements through labor migration and the loss of some traditional jobs.

All these evaluations support the requirement to improve the rules of legal law to relate to the new relationships imposed by the transformations of life in the digital ecosystem. Law plays a crucial role in defining how AI-based technologies are used, protecting individual rights and ensuring the ethical and legal environment for their development.

Therefore, the interaction of law with emerging technologies can represent an interdisciplinary field where legal and technological knowledge intersect. The law must regulate relations regarding the use of technologies but also labor law to ensure compliance with laws, individual rights and ethics.

We present some opinions that we consider benchmarks for future analysis and research in the field of law:

1. In the area of regulations in legislation: Governments around the world and a number of international institutions have begun to develop and adopt laws and regulations to manage the impact of emerging technologies on society. They mainly concern data privacy, responsibility for AI decisions, copyright, etc. Often, emerging technologies are cross-border, making regulations complex. International organizations such as the UN and other regional organizations are engaged in developing global norms and standards to govern the use of AI internationally.

2. In the area of legal liability: One of the main challenges related to AI is establishing liability if AI technology systems cause harm. Scenarios where autonomous decisions are taken by robots or in the event of damage caused by autonomous vehicles are considered. Moreover, the use of AI for legal purposes such as evaluating evidence or analysing legal cases can change judicial practice.

An important issue is accountability for actions and decisions made by AI systems. If AI causes harm or injustice it must be determined who is responsible: the developer, the user or the system itself. This may lead to the development of specific rules to determine responsibility. Moreover, the law must adapt to integrate these technologies into legal processes. The development of legal systems through AI must support case research, case law analysis and provide legal assistance.

3. In the field of data protection. The use of AI involves the collection and processing of large amounts of data. The European Union's General Data Protection Regulation (GDPR) sets strict standards for the protection of personal data and enforces penalties for breaching them. In addition, the data used to train AI technologies must be accurate and non-discriminatory. The law must regulate the process of data collection and use to prevent biases from being introduced into algorithms and to protect individual rights related to personal data. Protecting data privacy and security is essential.

4. To establish ethical norms in the use of emerging technologies. In particular, in the use of AI, special attention must be paid to ethical aspects (Ciupercă & Stanciu, 2022). Issues related to discrimination, bias and transparency in AI algorithms are important topics for which the law must regulate, through standards and certification, ethical evaluation techniques and transparency of systems.

5. In the field of intellectual property. Especially for AI products, copyright and intellectual property questions may arise. In the situation where this technology is used for the generation of creative content or for the development of technological innovations, it is necessary to establish clarifications regarding who has the right to own and exploit such a creation, what are the copyrights and what is patent ownership. But computer viruses are also creative products and can be generated by AI. In addition, increased use of AI may lead to increased disputes between parties requiring arbitration. Arbitration and alternative dispute resolution procedures can play an important role in resolving these disputes.

6. For automated contracts and negotiations. AI can be used to negotiate and enforce contracts, which raises questions about the validity and enforceability of these contracts in the eyes of the law. Additionally, to ensure compliance with the law and ethical standards, it is important that emerging technology systems are audited and provide a clear explanation of how they make decisions. Regulations can require transparency in AI algorithms and decision-making processes to avoid discrimination and bias.

7. Protection against discrimination. Civil rights and equality laws have significant application in the AI context. AI systems must be developed and used

in a way that does not perpetuate discrimination based on race, gender, sexual orientation or other protected characteristics.

8. Consumer protection. An important part of e-commerce is consumer protection. When it comes to AI in e-commerce and online services, consumer protection laws play a crucial role. The law must ensure that users benefit from transparency, correct and appropriate information to make informed decisions in online transactions, as well as protection against deceptive commercial practices.

9. In the area of international cooperation: Since AI is not limited to national borders, international cooperation is essential to develop common regulations and standards that facilitate the global use of information, AI and emerging technologies, to ensure the application of rules in an international context.

These are just some of the priority directions for which the legal framework must modernize through interaction with emerging technologies. For this, a transformation of education and training in the legal field is also necessary. Training specific to legal disciplines involves a high level of complexity. Lawyers and legal professionals must be prepared to address the new issues brought by emerging technologies and AI.

On a sectoral level, through the prism of the regulations of certain relationships specific to the implementation of emerging technologies in production chains, we consider the following aspects to be revealed, which support the need to modernize the law:

- The development of autonomous vehicles that have entered the European market since 2020 (European Parliament, 2019), raises a number of legal questions that require new regulations. For example, how is responsibility determined in the event of a road accident and what is the application of road traffic safety regulations.

- Automated systems and industrial robots are easy to find in various technological lines and replace personnel especially in critical functions for human health. Thus, self-regulating and self-administering systems that can make decisions and act independently produce new reports that need to be legally regulated, especially for how these robots perform tasks without human intervention. Who is responsible if problems arise? In addition, labor law must adapt in terms of the protection of the rights of human workers, the rules for replacing the work performed by human staff and the ways of professional training.

- Artificial intelligence can also be used to develop cyber-attacks. The situations in which such technologies are involved in military conflicts are no longer a secret of contemporary wars. It is becoming a rule that jurisdictional

issues will arise in international conflicts where actors use AI and other emerging technologies. Especially in offensive cyber operations information manipulation and disinformation are main techniques that rely on AI. International law must address these issues and develop effective methods of investigation and prevention, both for cyber-crimes and for specific actions of cyber terrorism. Protection against fake news or controlled content by these technologies must be regulated by tools to prevent and sanction these activities, ensuring the integrity of information and public discussion. In addition, legislative overlaps or regulatory gaps must be identified.

- The integration of emerging technologies can cause threats to privacy and freedom of expression. The defense of individual rights remains a crucial direction in the age of digital communication. Laws must balance the efficient use of technologies while protecting these rights.

We believe that those presented are only a few of the many aspects related to law and the interaction with emerging technologies. Collaboration between the legal and technology communities remains crucial to develop an appropriate social environment and address future challenges.

### III. THE SUPPORT OF THE NATIONAL INSTITUTE FOR RESEARCH AND DEVELOPMENT IN INFORMATICS – ICI BUCHAREST FOR THE MODERNIZATION OF THE LEGAL FRAMEWORK

Law and emerging technologies will continue to evolve in parallel, influencing each other. Their interaction will form an appropriate legal framework for the digital world of the future. In this sense, the National Institute for Research and Development in Informatics - ICI Bucharest must be considered a consistent support for the development of the national information society, having as its main mission support in research and innovation for the development of the knowledge-based economy and for better integration in the European space and international, of scientific research.

Over time, the institute's name has been associated with "premiere achievements" in Romanian informatics, among which we list (*ICI-Bucureşti, 2023*):

- development of the first national computer network;
- complete Internet connectivity through ".ro" domains registered with IANA (Internet Assigned Numbers Authority);
- the first digital library in Romania;
- the first Romanian consortium for the development of the Grid;
- the first algebra-oriented language and the first compiler for linear optimization;
- the first Romanian Grid site certified and included in the European EGEE profile infrastructure;

- the first IT project in the field of Cloud Computing for public institutions in Romania;

- the first Competence Center in the HPC field in Romania;

- the first center specialized in the field of Cyber Diplomacy;

- the first European course in the field of Cyber Diplomacy under the auspices of the European External Action Service (European Commission);

- pioneering the development and adoption of Blockchain technology for societal applications;

- the first center of Cyber – influence (CIASC);

- the first digital forensic mobile laboratory.

The results of scientific research are made available to those interested through articles and conferences appreciated at national and international level, being indexed in recognized databases. In recent years, ICI specialists have published more than 500 articles in specialized journals and proceedings, as well as more than 30 books or chapters in volumes, from the country and abroad. ICI is represented by former and current specialists in the Romanian Academy, the Academy of Scientists and the Academy of Technical Sciences.

ICI Bucharest is represented in over 20 national and 30 international professional associations. During its activity, ICI received on several occasions confirmation of the recognition of its level of excellence and ICI researchers were rewarded over time with prestigious national and international awards, awards of the Romanian Academy and Doctor Honoris Causa titles of some universities from the country and abroad.

ICI Bucharest publishes the following specialized magazines:

- Studies in Informatics and Control – SIC

- The Romanian Journal of Informatics and Automation (Revista Română de Informatică și Automatică – RRIA)

- Romanian Cyber Security Journal – ROCYS

- International Journal of Cyber Diplomacy – IJCD

Among the services and products provided by ICI Bucharest are:

1. The National Program Library (BNP - Biblioteca Națională de Programe) which is a digital library of software products launched in 2011. It offers information facilities and access to various software products available in Romania, being adapted to the current requirements of the new information society and to facilitate online registration of program products.

2. ICI-Learning is a learning platform (e-learning) developed in 2020, being a useful tool for professional training through courses held within the Continuing Professional Training and Training Centre.

3. ICIPRO is a Cloud Computing infrastructure for public institutions in Romania, being made available to public services offered to citizens. It was made

to streamline the acquisition and use of ICT (Information and Communications Technology) at the level of public institutions, to increase the transparency of the activity of public institutions and to facilitate interoperability between public electronic services.

4. Local network vulnerability scanning and alerting services through ICISOC. This is combined with the implementation of customized IT security policies at the level of detail, policies that can greatly raise the awareness level of employees, can increase the IT security level of the entity, at an almost symbolic cost compared to the range of services provided.

5. Smart device testing service for each field of activity regulated by legislation and requested by economic operators, distributors, manufacturers, importers of tested fiscal equipment.

6. The RoTLD Registry represents the official authority that administers the .RO top-level domains by creating, implementing and maintaining software systems, databases and an infrastructure necessary for the ".ro" domain to be present on the Internet.

7. Research - Development - Innovation activities in the field of Blockchain technology, Asset Tokenization and Trading Ecosystems. The services based on Blockchain technologies provided by ICI Bucharest are developed based on in-depth research studies of emerging technologies, understanding the complexity and advantages that these technologies bring to various fields of activity, such as: e-medicine, education, transport, legal, finance, business and many others.

8. ICI-SIOC (Smart Integrated Operations and Control) is a complex solution for monitoring infrastructures, applications and IT services, providing support for AIOps with the aim of ensuring a high level of reliability, performance, security and information intelligence. Within the center IT experts, investigators and/or lawyers can carry out collaborative work for activities related to the field of computer forensics.

Last but not least, ICI organizes, is a partner or guest at a series of scientific events of international and national, professional or sectoral interest.

Among these, the cyber diplomacy conference, the International Conference on Cyber Diplomacy, this year is in its second edition. The event brings together various decision-makers and managers from the public and private sector, exponents of the institutional and diplomatic environment, academic and security experts, other relevant specialists for the fields in which cyber technologies are implemented. During the conference, topics are addressed about recent challenges and trends in the field of cyber security at the global level, about the role of diplomacy in generating common advantages through dialogue and a collective strategy. The current edition of the conference facilitated the approach

of topics of great interest such as: the analysis of the evolution of cyber threats, cross-border cyber-crime, internet governance, regulations in the cyber field, the impact of fake news on cyber diplomacy and many others.

Last but not least the international conferences that have become events with tradition, organized in partnership with other prestigious institutions under the name of Virtual Learning - ICVL (this year being at the 18th session) and the National Virtual Education Conference - CNIV (this year being at 21st session with international participation), bring together important representatives of Romanian education, offering an appropriate framework for the exchange of experience to actors involved in education, creating opportunities for future joint projects.

## CONCLUSIONS

*Concerns regarding the regulation of the use of emerging technologies and AI pose challenges both to the development of digitized technologies and to the contemporary legal system. The harmonization of norms and laws is the subject of numerous international meetings and discussions in various appropriate domestic and regional environments, with a view to building a common vision for a governance of the digital economy in accordance with democratic values, based on reliable emerging technologies. In this context, steps are being taken in Romania towards alignment with European legislation and international standards and good practices. They address issues mainly related to physical and cyber security for technical equipment and systems, establishing the model of a technical and organizational framework for the implementation of certification schemes and for accreditation regarding cyber security.*

*By Government Decision no. 1.321/2021, Romania's cyber security strategy for the period 2022-2027 was approved, as well as the action plan for its implementation. The document, based on an updated vision of the evolution of the cyber security issue, identifies five objectives of strategic importance, among which the achievement of a consolidated normative and institutional framework stands out.*

*In terms of the organization of cyber security activities at the national level, the general cooperation framework represented by the National Cyber Security System (SNSC - Sistemul Național de Securitate Cibernetică), coordinated by the Cyber Security Operative Council (COSC - Consiliul Operativ de Securitate Cibernetică), was defined. It brings together, unitarily coordinates and ensures cooperation at the level of all national actors in order to know, prevent, deter and respond to cyber threats to Romania. The main actors are the public authorities with competences in the matter, actors from the non-governmental, professional and business associative environment.*

*As is known, the Supreme National Defense Council (CSAT - Consiliul Suprem de Apărare a Țării) is the authority that strategically coordinates the*

*activity of the SNSC. The National Cyber Security Directorate established by GEO no. 104/2021 (Mof I no. 918/24.09.2021) represents an interface of the COSC member institutions for the cooperation of the listed actors with civil society, the private and academic environment, constituting an optimal framework for the creation and development of effective partnerships in the field of cyber security.*

*It is important to note that due to the complexity and interdisciplinary nature of the cyber security field, cooperation between different bodies, authorities and agencies is crucial to identify appropriate approaches to specific challenges in order to further develop the industry and related economies.*

*We are convinced that the entire legislative, national, European and international system will evolve and adapt continuously to identify and apply the best solutions in order to reduce the decision-making gap, to ensure the best conditions for the physical and cyber security of citizens, as well as for the maintenance of fair conditions for businesses, with a view to the economic development of all countries.*

*Through what has been presented, we want to reinforce the convictions that ICI Bucharest, like other professional structures, is actively working to improve the digital environment for the benefit of citizens in order to identify solutions and applications designed to effectively protect online users, to ensure cyber security and to facilitate the exchange of information in conditions of real cyber security.*

## BIBLIOGRAPHY

1. Boroi G. & Anghelescu C.A. (2021), Civil Law Course, General Part, 3rd Ed., Revised and Added [*Curs de Drept Civil, Partea generală*, Ed. A 3-a, revizuit și adăugat], Ed. Hamangiu, Bucharest;

2. Ciupercă E. M. & Stanciu A. (2022), *Social networks-based alt-metrics and the unethical use of AI*, International Conference on Virtual Learning, ISSN 2971-9291, ISSN-L 1844-8933, vol. 17, 2022. https://doi.org/10.58503/icvl-v17y202 214 visited at 20.10.2023;

3. Ciupercă E.M., Cîrnu C. E., Stanciu A. & Cristescu I., (2022), *Leveraging socio-cultural dimension in cyber security training. 14th International Conference on Education and New Learning Technologies*, 4-6 July 2022, Palma, Spain, EDULEARN2022 Proceedings, 5242-5248, ISBN: 978-84-09-42484-9, ISSN: 2340-1117, DOI: https://dx.doi.org/10.21125/edulearn.2022.1239, ISI conference visited at 20.10.2023;

4. Conferința Națională de Învățământ Virtual [National Virtual Education Conference] – CNIV 2023, https://cniv.ro/ visited at 30.10.2023;

5. Dinu, M.-Șt. (2022), *Domeniul cibernetic – Aspecte cu impact în evaluarea stării de securitate a statelor [*The cyber domain – *Aspects with impact in the*

*assessment of the security state of states]*, Military Science Review, V3, no. 68, https://www.ceeol.com/search/article-detail?id=1079407 visited at 21.10.2023;

6. ICI-Bucharest (2023), https://www.ici.ro/ro/istoric/ visited at 23.10.2023
International Conference on Virtual Leraning – ICVL (2023), https://icvl.eu/ visited at 30.10.2023;

7. Mihăilescu, S. L. Th. (2023), *Suport de curs pentru disciplina: Drept constituţional şi instituţii politice [Course support for the discipline: Constitutional law and political institutions],* Ecological University of Bucharest, Law Faculty, ;https://www.ueb.ro/drept/ebiblioteca/files%202022/DREPT%20 CONSTITUTIONAL.pdf visited at 20.10.2023

8. European Parliament (2019), *Vehiculele autonome sunt pe cale să devină realitate în UE [Autonomous vehicles are about to become a reality in the EU]*, https://www.europarl.europa.eu/news/ro/headlines/economy/20190110STO23102 /vehiculele-autonome-sunt-pe-cale-sa-devina-realitate-in-ue visitied at 27.10.2023;

9. Vevera A.V. (2019), *Reglementări legislative cu privire la securitatea cibernetică [Legislative regulations regarding cyber security],* Ed. ICI, București. World Economic Forum (2023), *The Future of Jobs Report 2023*, https://www.weforum.org/publications/the-future-of-jobs-report-2023 visited at 23.10.2023.