SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N°. 1 (2025), pp. 17-30

NEW DIMENSIONS OF LEGAL RESPONSIBILITY AND LIABILITY IN THE ERA OF NEW TECHNOLOGIES

E. ANGHEL

Received 14.11.2025; accepted 16.12.2025
First online publication:16.12.2025
DOI: https://doi.org/10.55516/ijlso.v5i1.279

Elena ANGHEL
Lecturer PhD at the Nicolae Titulescu University of Bucharest, Faculty of Law Bucharest, Romania
E-mail: elena.anghel@univnt.ro
ORCID ID: https://orcid.org/0009-0003-7157-5418

Abstract

In the era of accelerated digitalization, characterized by advanced technologies such as artificial intelligence and system automation, traditional legal concepts and principles require urgent adaptation and reinterpretation. Responsibility and legal liability acquire new dimensions: while in classical law liability was closely conected to human will and action, today we often face unprecedented situations in which decisions originate from autonomous systems or opaque algorithms. The attribution of fault and the establishment of liability represent major challenges. Who is responsible when an erroneous decision is generated by an automated system? How can fault be determined if the consequences cannot be associated with a person responsible for them? Can autonomous robots themselves be considered legal subjects? How is liability defined in the case of artificial intelligence generating harmful content?

This study aims to analyze how the era of new technologies compels the law to reconfigure fundamental concepts such as responsibility and liability—concepts increasingly disconnected from human will. As technology evolves at an unprecedented pace and new, complex challenges emerge daily from advanced and autonomous artificial intelligence systems, while the normative framework develops timidly at the European level, it becomes the judge's particularly difficult task to find solutions to these cases and to act with great caution, given the absence of precedents and the continuously changing evolution.

Key words: *responsibility and liability; artificial intelligence; Internet of Things; unprecedented challenges; automated systems; fault attribution; European legislative benchmarks.*

INTRODUCTION

I. RESPONSIBILITY AND LIABILITY: THE CLASSICAL PARADIGM

In its moral dimension, responsibility is essentially an attribute of human personality, being closely conected to the degree of development of self-awareness. Endowed with reason and conscience, the human being is free to choose, to decide, and to act. Only the autonomous human individual is responsible and therefore liable. Such an individual is aware of values, understands and internalizes them, then chooses among them and translates them into action. In the application of law, legally enshrined values become reference points for the individual's personality which, endowed with responsibility, will orient and assess his behavior according to the standards they contain.

For the functioning of legal liability as a specific institution of law to be connected with the general aims of the legal system, it is necessary to maintain the belief that the law can create in the consciousness of its addressees a sense of responsibility (*N. Popa, E. Anghel, C. Ene-Dinu, L. Spătaru-Negură, 2023, p. 246*).

Law becomes binding in relations among individuals not as a necessary result of the coercive power of the state, but through the adherence of the members of society to its norms. Therefore, the law must be accepted both in terms of values and norms by the members of society (*E. Anghel, 2025, p. 28*). But while other values accompany the human being from birth—freedom-value, equality-value, - responsibility must be cultivated and educated; it is not innate. "The human individual is not born with a fully formed responsible personality (…), but with the potential to be responsible, a potential which is indeed realized during his psychosocial development as a subject knowledgeable of himself and of the other" (*Gh. Mihai, 2006, p. 34*).

Analyzing its legal dimension, Dumitru Mazilu defines responsibility as "an intrinsic coordinate of human behavior, playing a decisive role in the conscious and freely consented fulfillment of legal norms and in preventing breaches of the law" (*Mazilu D., 2007, p. 144*).

In this context, I argued in a previous study (E. Anghel, 2015, p. 364-370) that the individual who is cognitively and volitionally free is responsible for his acts and only to that extent can be held liable. Social liability cannot be detached from responsibility, which constantly relates to values; the breach of value-bearing norms (which amounts to insufficient assimilation, internalization, and completion of self-awareness) triggers the liability of the person concerned.

Etymologically, the term "responsibility" derives from the Latin *spondeo*, which in Roman law designated the debtor's solemn obligation toward the creditor to fulfill the performance assumed by contract. Legal responsibility is an institution through which the legislator expresses the vocation for legal liability of certain persons for potential acts and deeds committed.

Legal liability, in its classical paradigm, is based on the fulfillment of several requirements: the premise is the existence of a legal subject - the human endowed with discernment and legal capacity, - who commits an unlawful act with the form of fault required by law, thus making it possible to establish a causal link between the act and the damage. Are these assertions still valid today, in the context of the unprecedented evolution of new technologies? Is the human dimension still a *sine qua non* condition of liability? Can responsibility exist without consciousness, without reference to values? And, above all, can an entity that lacks perception of the norm be sanctioned?

The transformations brought about by new technologies require a profound reevaluation of the concepts of responsibility and liability in law. Faced with autonomous entities such as artificial intelligence, legal liability can no longer be viewed exclusively through the lens of direct human action, but instead demands new normative mechanisms adapted to technological reality.

II. RECONFIGURING TRADITIONAL CONCEPTS IN THE AGE OF NEW TECHNOLOGIES

Artificial intelligence, autonomous robots and algorithmic decision-making challenge the traditional premises of human imputability and generate a genuine crisis of liability and fault. Although some artificial intelligence technologies have existed for more than 50 years, today the availability of enormous quantities of data and new algorithms give rise to major challenges. Society as a whole is receptive to the new technologies of the future because they make life easier (*E.E. Ștefan, 2025*).

Artificial Intelligence (AI) refers to a set of technologies designed to develop systems capable of simulating and performing functions normally associated with human intelligence. In other words, AI is the ability of a machine or program to think, learn, reason, and make decisions in order to solve problems or carry out tasks that previously required human intelligence.

Artificial intelligence involves the development of algorithms and models that enable machines to perceive their environment, process information, and act autonomously or semi-autonomously, relying primarily on machine learning. Algorithms are trained on very large volumes of data, and the system learns patterns and rules from the training data in order to provide predictions or make decisions.

Types of artificial intelligence include virtual assistants, image analysis software, search engines, voice and facial recognition systems, as well as embedded AI: robots, autonomous vehicles, drones, and the Internet of Things.

Beyond the many benefits AI can bring to our lives, it also raises significant concerns about the harm these systems may cause to essential values such as life, health, and property, particularly since such harm is often extremely difficult to prove, and liability challenging to establish.

Regarding the *Internet of Things (IoT)*, it is defined as a global infrastructure of the information society designed to provide advanced services through the interconnection of physical and virtual objects (*Recommendation ITU-T Y.2060*). IoT valorizes the identification, processing and communication of data to deliver services to various applications, while respecting security and confidentiality requirements. In the future, IoT aims to integrate technologies such as machine-to-machine communications, autonomous networks, cloud computing, artificial intelligence, and robotics - to develop applications such as intelligent transportation, smart grids, e-health or smart homes. These systems will combine connectivity and autonomy to operate with minimal human intervention, improving their performance through continuous learning.

The benefits of adopting AI systems can be extraordinary for society, fostering economic development and strengthening the EU's innovation capacity and global competitiveness. For example, in health care, researchers are studying how AI can analyze large amounts of medical data to identify patterns that could lead to new medical discoveries and improved patient diagnosis. A notable example is an AI program designed to respond to emergency calls and recognize cardiac arrest during the call more quickly and more accurately than human dispatchers. Another example is KConnect, co-funded by the EU, which develops multilingual text-search services to help people find the most relevant available medical information.

Despite this potential, however, in certain cases the specific characteristics of some AI systems can generate significant risks regarding user safety (including physical safety) and fundamental rights. One of the most difficult issues concerns the attribution of liability for decisions made by automated systems, given that the decision belongs to an algorithm, with no causal link that can be established between human intention and the outcome. The enormous volume of data involved, as well as the dependence on algorithms and the opacity of the AI decision-making process, make it difficult to predict the behavior of an AI-equipped product or to understand the causes that led to the harm.

Balancing the benefits alongside the risks posed by new technologies, this study argues for the reinterpretation and adaptation of traditional legal concepts, in a context where the present challenges us to decide whether algorithms, robots and digital entities that autonomously produce legal effects - beyond human will - may themselves become subjects of law. The wrongful act may now consist in a complex and opaque (black-box) decision-making process that generates results which can no longer be associated with human intervention. Fault can no longer be determined in the traditional sense of intent or negligence, but rather as the decision of an autonomous system that produces those results. As for the causal relationship between the act and the damage, it becomes extremely difficult to isolate and determine the level of involvement of the programmer, the operator, the user, and the autonomous system itself, within this complex network of

interacting agents. Who is liable when a decision causes harm? Is it the programmer who designed the algorithm, the system provider, or the human operator behind the algorithm - the one who validated the harmful outcome?

In complex technological networks characterized by multiple interdependencies, when damage results from the interaction of dozens of software modules, servers, automatic updates and external factors, identifying a single culpable actor becomes almost impossible. The digital environment is marked by *"liability without fault"* or *"distributed liability",* where the focus shifts away from fault and toward the fair allocation of risk among the actors involved.

Distributed liability implies a joint assumption of legal consequences, with each participant in the technological chain bearing part of the damage according to their role and level of control exercised.

Although innovative, this model raises questions regarding its compatibility with traditional civil-law principles, which require individualized liability and the personal nature of fault. In Romanian law, such a paradigm demands a rethinking of tort liability and perhaps even the introduction of an autonomous legal regime for digital liability.

In the absence of a special legal framework for artificial intelligence, damages caused by new technologies fall under the following Romanian regulations:

1. *Product liability for defective products*, governed by Law no. 240/2004 on the liability of producers for damage caused by defective products, republished, which transposes Directive 2024/2853. This regime is considered efficient for AI, as it makes no distinction between contractual and tort liability and applies regardless of whether the victim is a third party or a contracting party. However, the challenge remains proving the defect, particularly in the case of opaque algorithms (*M. Duțu, 2025*).

2. *Tort liability based on fault:* proving fault is difficult or even impossible in some cases due to the opacity and complexity of AI systems.

3. ***Contractual liability*** applies when the damage results from a contract, but its effectiveness is often hindered by the burden of proof.

4. ***Liability for things*** may apply if the system/product that caused the damage can be considered a "thing" that triggers liability for the owner under whose control it is held.

None of these regimes fully correspond to the specific features of artificial intelligence systems, as their opacity, connectivity, complexity and autonomy hinder the establishment of causation and the attribution of liability to the actors involved. Nevertheless, fault-based liability would remain the most feasible solution, both in tort and in contract liability. In the future, the Romanian legislator may opt to introduce a new special form of liability - liability for damage caused by artificial intelligence systems.

Consequently, since Member States cannot keep up with the pace of technological evolution, a unified legislative approach at EU level is absolutely necessary, one capable of establishing common European standards for citizens and businesses and ensuring legal certainty across the Union.

According to assessments by domain specialists, since 2010 more than 600 reports, frameworks, and public or private standards related to artificial intelligence and robotics have been issued. We are facing a complex, innovative, and crucial process in which the pace of regulation can scarcely keep up with the speed of technological innovation, and its intrinsic nature undergoes major transformations in the logic of expressing specificity and in the adequacy of the legal response to the implications of a major scientific and technological revolution (*M. Duțu, 2025, p. 11*).

III. EUROPEAN LEGISLATIVE LANDMARKS

The consequences and challenges of artificial intelligence transcend borders; therefore, international cooperation is essential, as AI is considered a central element of society's digital transformation. As AI has become a priority, the European Union is focused on promoting trustworthy artificial intelligence that is human-centred and grounded in ethical principles. In cooperation with international partners, the EU seeks to ensure the responsible governance of AI, in line with the values it upholds.

In 2017, during debates in the European Parliament, the possibility of granting legal personality to autonomous robots was examined, through the regulation of the concept of *"limited electronic personality."* This entailed a legal fiction: treating autonomous robots as "electronic persons" with limited legal personality for the purpose of establishing liability for the damage they cause. Although such a legal fiction would allow direct liability to be attributed to the autonomous system, the proposal was strongly criticised by experts, who argued that granting AI legal personality may dilute human responsibility (i.e., that of developers, manufacturers or users). For this reason, the European Union did not adopt this concept, opting instead for an approach based on clear human liability and traceability of algorithmic decisions.

Subsequently, in its Resolution of 20 October 2020 containing recommendations to the Commission on a civil liability regime for artificial intelligence, the European Parliament stressed that all activities, devices or processes - physical or virtual - directed by AI systems may technically be the direct or indirect cause of harm, but are nonetheless almost always the result of actions taken by someone who built, deployed or interfered with those systems. Therefore, the Parliament stated that it is not necessary to grant legal personality to AI systems: *"Any necessary modification of the existing legal framework should begin by clarifying that AI systems have neither legal personality nor human consciousness and that their sole purpose is to serve humanity."*

To effectively harness the advantages of AI while preventing potential misuse, the European Parliament has emphasised the need for uniform legislation, grounded in the principles and values of the Union, applicable to all AI systems. Each Member State may adapt its liability rules for certain actors or make them stricter for certain activities, without a complete overhaul of national legislation being required. What is essential is that liability regimes be adapted so that individuals suffering harm or whose property is damaged can be compensated.

Although the opacity, connectivity and autonomy of AI systems may in practice make it very difficult or even impossible to establish a causal link between the damage caused by AI and the human contributions involved, the European Parliament considers that, in line with generally accepted concepts of liability, it is still possible to hold accountable the various persons involved in the value chain who create, maintain or control the risks associated with an AI system.

In June 2024, the European Union adopted the world's first comprehensive AI rules. The *Artificial Intelligence Act (AI Act, 2024)* will become fully applicable 24 months after entry into force, though certain provisions, such as the prohibition of AI systems posing unacceptable risks, apply earlier.

The issue of liability has been addressed at EU level by proposing a system for classifying AI according to the risks involved. AI systems used in different applications are analysed and classified based on their level of risk to users.

AI applications involving *unacceptable risks* are prohibited within the EU, such as cognitive-behavioural manipulation of individuals or vulnerable groups (for example, voice-activated toys encouraging dangerous behaviour in children) or biometric identification and categorisation of individuals, including facial recognition in public spaces.

AI systems that negatively affect safety or fundamental rights are classified as *high-risk*, divided into two categories. The first includes AI systems integrated into products covered by EU product safety legislation (toys, aviation, machinery, medical devices, lifts).

The second concerns AI systems in specific fields that must be registered in an EU database, such as: education and vocational training; employment, worker management and access to self-employment; law enforcement; migration, asylum and border control management; and assistance in interpreting and applying the law.

All high-risk AI systems will be evaluated both before being placed on the market and throughout their lifecycle. Citizens will have the right to lodge complaints with national authorities concerning AI systems. AI-generated or AI-modified content - including images, audio and video (e.g., deepfakes), must be clearly labelled as AI-generated so that users are aware of this.

The AI Act establishes a two-tier governance system, where national authorities are responsible for supervising and ensuring compliance of AI systems, while the EU oversees the regulation of general-purpose AI models.

Within this framework, the AI Act underscores *the principle of human oversight*, requiring risk-assessment mechanisms to prevent arbitrary or discriminatory algorithmic decisions. The aim is to establish "distributed algorithmic liability," whereby each actor involved in the design and use of AI assumes a clearly defined share of responsibility.

Algorithmic liability seeks to ensure public trust in AI technologies, protect fundamental rights (especially data protection and the right to fair treatment), and prevent the impunity of automated decision-making. In my view, algorithmic liability represents the means through which the law seeks to adapt traditional principles of civil liability to the digital age, ensuring that the use of algorithms remains subject to control and does not eliminate human accountability.

The Parliament's priority has been to ensure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally sustainable. AI systems must be subject to human, not automated, oversight, in order to avoid harmful outcomes.

The European Parliament considers that the existing liability regimes of the Member States based on fault-based civil liability (subjective liability) provide, in most cases, a sufficient level of protection for individuals who suffer harm caused by the intervention of a third party, such as a hacker. Accordingly, it takes the view that the introduction of new legal rules on civil liability into domestic law is necessary only in specific circumstances, for example when the third party cannot be identified or lacks financial resources.

An analysis of the principles established by European regulations reveals two possible approaches to designing liability: *liability based on objective risk*, which entails the responsibility of the party placing an autonomous system into circulation and assuming the consequences of any damage caused, irrespective of fault; and *algorithmic, collective liability*, which is proportionally distributed among the programmer, operator, user and the technological platform.

Algorithmic liability requires identifying the persons or entities that may be held accountable for harm caused by the use of an algorithm (developers, providers, users, or entities implementing the system), while complying with several requirements: *transparency* - the algorithm must be sufficiently clear to allow understanding of how it makes decisions; *traceability of decisions* – it must be possible to reconstruct the system's decision-making logic so that the source of the error leading to the damage can be determined; *human responsibility* – even if the decision is taken by an autonomous algorithm, final liability rests with an identifiable human actor; *legal remedy* – individuals affected by an algorithmic

decision must have access to mechanisms for challenging and obtaining redress for the harm.

In the field of product safety, the European Commission is concerned with addressing the absence of provisions relating to new digital risks, such as cyber-threats that may compromise user safety, or the difficulty of predicting the behaviour of AI-based products (the "black-box effect"), which complicates tracking and understanding the causes of a defect.

At the Union level, the provisions on product safety and product liability aim to create a single market for goods, intended to ensure a high level of safety and provide compensation for damage arising from defective products. (The report *"Liability for Artificial Intelligence and Other Emerging Digital Technologies"* may be consulted at[1]:

Another benchmark in the field of liability is Council Directive 85/374/EEC of 25 July 1985 (the Product Liability Directive), which has proven for more than 30 years to be an effective instrument for compensating damage caused by defective products. Consequently, it should also be applied in cases where a party suffering harm or damage brings a civil liability action against the manufacturer of a defective AI system.

The Product Liability Directive offers a level of protection that national fault-based liability regimes alone do not provide. It introduces a system of strict liability for producers for damage caused by a defect in their products. In cases involving physical injury or property damage, the injured party is entitled to compensation if they prove the damage, the product defect (that is, that the product failed to provide the safety the public is entitled to expect), and the causal link between the defect and the damage.

Unharmonised national regimes provide fault-based liability rules under which victims of harm must prove the fault of the responsible person, the damage, and the causal link between the fault and the damage in order to successfully initiate a liability claim.

Furthermore, national liability regimes offer victims of damage caused by products and services several parallel claims for compensation, based on either fault or strict liability. These claims are often directed against different responsible persons and are subject to different conditions. For example, a victim involved in a car accident usually has a strict liability claim against the owner of the vehicle (i.e. the person who concluded the compulsory motor liability insurance), a fault-based claim against the driver under national civil law, and a claim under the Product Liability Directive against the manufacturer if the car had a defect.

[1] https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en

However, the features of new technologies make it difficult to establish the sequence of events leading back to the human behaviour involved in causing the damage, with the result that a fault-based claim under the national tort regime would be very hard to prove, leaving victims inadequately compensated.

With regard to civil liability, the challenge lies in ensuring that victims of harm caused by artificial intelligence or the Internet of Things benefit from protection as effective as that relating to traditional technologies. Thus, in complex environments involving multiple actors (including software), in order to identify the responsible party and establish the causal link between a defect and the damage suffered, the possibility of reversing the burden of proof in favor of the victim is analyzed, with liability arising as a result of the failure to comply with specific legal obligations regarding cybersecurity.

CONCLUSION

The potential of new AI-based technologies and the benefits they can bring to humanity are immense, with the capacity to improve our lives in almost every field, from transportation, education and assistance for vulnerable individuals to global challenges such as climate change, healthcare, nutrition and logistics. Artificial intelligence promises new breakthroughs in the treatment of chronic diseases, epidemic prediction, combating climate change and anticipating cyber-threats. In terms of safety, autonomous vehicles can significantly reduce accidents caused by human error.

Yet, beyond these opportunities, new technologies also pose the risk of serious harm to legally protected interests, both material and non-material. We are faced with new challenges regarding product safety and liability, such as connectivity, autonomy, data dependency, opacity, complexity of products and systems, and software updates.

The development of AI-based technologies is so dynamic that it requires a clear and predictable legal framework, capable of providing citizens with protection and trust in the face of these new digital risks. The opacity of these technologies, the multitude of actors involved and the vulnerability of AI systems to cyberattacks sometimes make it impossible to identify the person who controls the risks associated with the use of an AI system or the individual who caused the damage. The constant efforts of countries to increase the level of domestic cybersecurity are obvious in this age, when the latter cannot be separated from European and world cyber security (Iancu, E.-A., Tuşa, E., Iancu, N., Simion, E., Moise, A.-C., 2023, p. 366). Moreover, in such an unrestrained world, AI systems may at times be used precisely to undermine human dignity or European values by enabling the creation of lethal autonomous weapons, the unwarranted surveillance of individuals, or biased decision-making in areas such as health insurance (for an analyze of the crime, especially those that can be committed

through information systems referring to the decade of digitization, see Cîrmaciu, D., Iancu, E.-A., 2025, pp. 265-277).

Artificial intelligence can also be used to influence public perception and manipulate information for political, economic, or social purposes. In the context of national security, it may be employed to: generate and disseminate large-scale fake news, through natural language processing and neural networks capable of producing highly convincing fabricated messages and articles; create deepfakes - AI technologies designed to produce false videos and audio recordings that can generate propaganda materials almost indistinguishable from reality; enable facial recognition - AI-powered systems allowing the tracking of individuals in public and private spaces, raising serious concerns regarding privacy and civil liberties; facilitate behavioural surveillance - algorithms capable of analysing online behaviour to predict actions or to influence them through excessive content and advertisement personalisation (R. N. Lungeanu, 2025, p. 7).

Another challenge arises from the fact that AI-based products and services will interact with traditional technologies, resulting in increased complexity in matters of liability. For example, autonomous vehicles will coexist with traditional ones for a certain period. A similar complexity of interacting actors will occur in some service sectors (such as traffic management and healthcare), where partially automated AI systems will support human decision-making.

Given these risks, it is essential to ensure that new digital products operate safely and that, when harm occurs, injured parties receive compensation. The actors involved in the AI system must be held liable for the damage caused, in accordance with general principles of liability, according to which the person who creates or presents a risk to the public is responsible when that risk results in harm or injury.

A human-centred approach to AI means ensuring that AI applications comply with fundamental rights legislation. By integrating requirements of accountability and transparency into the development of high-risk AI systems and improving enforcement capacities, these systems will inspire the necessary trust among citizens, as underlined by the European Parliament in 2020, when it adopted the Resolution containing recommendations to the Commission on a civil liability regime for artificial intelligence.

The European Parliament has emphasised that any forward-looking legal framework on civil liability must inspire confidence in the safety, reliability, and consistency of products and services - including digital technology - so as to ensure a fair and effective level of protection for potential victims of harm, while at the same time allowing sufficient room for businesses, especially small and medium-sized enterprises, to develop new technologies, products or services.

These liability challenges must be addressed to guarantee the same level of protection for victims of AI-related harm as for those harmed by traditional

technologies, while maintaining a balance with the need for technological innovation. This will help foster trust in new emerging digital technologies and generate investment stability.

We cannot slow down the evolution of new technologies, nor can national legislation keep pace with such rapid developments, but we can remain actively engaged in regulating the use of artificial intelligence, participating in decision-making processes and monitoring its impact. It is essential for the law to preserve its protective and balanced function by identifying clear solutions for the distribution of responsibility among developers, users, institutions, or even digital entities. Ultimately, only through continuous dialogue between law, technology, and ethics can we shape a functional and equitable legal framework for the age in which we live.

BIBLIOGRAFIE

1. E. Anghel, *Principiile dreptului*, Universul Juridic Publishing House, Bucharest, 2025.
2. E. Anghel, *The responsibility principle*, in Proceedings of the Challenges of the Knowledge Society Conference (CKS) no. 5/2015, „Nicolae Titulescu" University Publishing House, Bucharest, 2015, https://cks.univnt.ro/cks_2015.html.
3. S.G. Barbu, A. Muraru, V. Bărbățeanu, *Elemente de contencios constituțional*, C.H. Beck Publishing House, Bucharest, 2021.
4. M. Bădescu, *Teoria generală a dreptului*. *Curs universitar*, 7th edition, revised and added, Hamangiu Publishing House, 2022.
5. I. Boghirnea, *Internet and artificial intelligence – as law configuration factors*, in Journal Legal and Administrative Studies, Supplement 2024, Publishing House C.H. BECK Bucharest 2024.
6. Cîrmaciu, D., Iancu, E.-A., *Challenges in the Changing World of Labor Relations. Human Resources, Finance and Crimes in the Decade of Digitalization*, published in Changes and Innovations in Social Systems, coordinated by Sarka Hoskova-Mayerova, Cristina Flaut, Daniel Flaut, Pavlina Rackova, Editura Springer Nature, Berlin, Germany, p. 265-277, 2025, DOI: https://doi.org/10.1007/978-3-031-43506-5
https://link.springer.com/chapter/10.1007/978-3-031-43506-5_15.
7. M.C. Cliza, *A Topical Discussion-Digitalisation of Public Administration and Public Services in Romania*, Perspectives of Law and Public Administration 14, no. 2 (June 2025): 283-293, DOI: 10.62768/PLPA/2025/14/2/04
8. I. Craiovan, *Teoria generală a dreptului*, the Military Publishing House, Bucharest, 1997.
9. M. Duțu, *Elemente de dreptul inteligenței artificiale* (Elements of artificial intelligence law), Universul Juridic Publishing House, București, 2025.

10. M. Duțu, *Probleme și dileme privind regimul juridic al răspunderii civile pentru inteligența artificială: O analiză detaliată*, 2025, https://www.wolterskluwer.com/ro-ro/expert-insights/raspunderea-ai-1
11. C. Ene-Dinu, *The impact of GDPR on forensic idenntification technologies based on artificial intelligence for facial recognition, fingerprints and DNA profiles comparison in modern investigations*, Romanian Journal of Forensic Science, 2025, Vol 26, Issue 141.
12. Iancu, E.-A., Tușa, E., Iancu, N., Simion, E., Moise, A.-C., *Preventing computer crime by knowing the legal regulations that ensure the protection of computer systems*, în Tribuna Juridică nr.3./2023, https://www.tribunajuridica.eu/arhiva/anul13v3.html
DOI: 10.24818/TBJ/2023/13/3.03
13. R.N. Lungeanu, *The new social reality: artificial intelligence and the necessity of aligning national legislation with societal evolution*, Vol. 5 No. 1 (2025): IJLSO DOI: https://doi.org/10.55516/ijlso.v5i1.258
14. M. Niemesch, *Teoria generală a dreptului*, ed. 3rd, revised and added, Hamangiu Publishing House, Bucharest, 2019.
15. E. Magrani, *New perspectives on ethics and the laws of artificial intelligence., in , Journal on internet regulation Volume 8 | Issue 3* DOI: https://doi.org/10.14763/2019.3.1420
16. D. Mazilu, *Tratat de teoria generală a dreptului*, 2nd edition, Lumina Lex Publishing House, Bucharest, 2007.
17. Gh. Mihai, *Fundamentele dreptului, Teoria răspunderii juridice*, vol. V, C. H. Beck Publishing House, Bucharest, 2006.
18. N. Popa, E. Anghel, C. Ene-Dinu, L. Spătaru-Negură, *Teoria generală a dreptului. Caiet de seminar, 4th edition*, C.H. Beck Publishing House, Bucharest, 2023.
19. The National Strategy on Artificial Intelligence, SIPOCA code 704, implemented by the Authority for the Digitalization of Romania for 2024–2027 (NS-AI), approved by Government Decision no. 832/2024 and published in the Official Gazette no. 730 of 25 July 2024, https://www.adr.gov.ro/wp-content/uploads/2024/06/Strategia-Nationala-pentru-Inteligenta-Artificiala.pdf.
20. E.E. Ștefan, *Vulnerabilities of new technologies in the work of public authorities and the need for cyber security*, in Sciencia Moralitas 10 (1): 376, 2025, DOI: 10.5281/zenodo.16415586
21. Council Directive 85/374/EEC of 25 July 1985 (the Directive on liability for defective products), published in OJ L 210, 7.8.1985.
22. Law no. 240/2004 on the liability of producers for damage caused by defective products, republished, in the Official Gazette no. 313 of 22 April 2008.

23. The report 'Liability for Artificial Intelligence and Other Emerging Technologies'. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.
24. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized 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 Regulation) [Official Journal of the European Union, 12.07.2024].
25. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060
26. https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52020IP0275
27. https://www.europarl.europa.eu/topics/ro/article/20230601STO93804/legea-ue-privind-ia-prima-reglementare-a-inteligentei-artificiale
https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en).