Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 17 (1), 2025
pp. 102 - 110

Legal Liability for the Use of Artificial Intelligence in the Healthcare Sector

[1]Bourayou mohammed Yacine, [2] Founas souhila

[1]Badji Mokhtar – Annaba University Algeria

mohamed.yacine-bourayou@univ-annaba.dz

[2]Badji Mokhtar – Annaba University Algeria

Souhila.founes@univ-annaba.dz

Submitted on: January 6, 2025 Accepted on: March 10, 2025 Published on: April 15, 2025

Abstract:
The present study aims to shed light on the legal liability associated with the use of artificial intelligence (AI) in the healthcare sector by examining both civil and criminal liability related to the deployment of medical robots. The study concluded that AI systems and robots are programmed to perform assigned tasks and objectives autonomously; as such, they are often incapable of responding effectively to unforeseen situations, which may result in undesirable or unlawful outcomes. Consequently, developers, operators, or users of AI technologies may bear responsibility for negligence or lack of competence. The study recommends the establishment of a comprehensive set of guidelines for the use of AI in healthcare, addressing issues of safety, privacy, non-discrimination, and accountability.

Keywords: Artificial Intelligence, Legal Liability, Healthcare Sector, Guidelines.

Introduction

The medical field is undergoing rapid and unprecedented transformations, driven by the integration of modern technologies, including a wide range of advanced devices and equipment. While these innovations enhance healthcare delivery, they may also pose significant risks to individuals' rights and physical safety.

The right to life, health, and bodily integrity, as well as the prohibition of harm, are among the most fundamental human rights safeguarded by both religious principles and legal frameworks. In today's world, employing advanced technological tools to protect public health has become a necessity. However, while the use of technology—particularly artificial intelligence (AI)—has introduced major efficiencies for both patients and medical professionals, it has also raised new concerns and potential threats to these protected rights.

The healthcare sector now stands as one of the primary beneficiaries of intelligent technologies, with AI offering significant advancements in diagnostic accuracy, treatment planning, and beyond. This growing reliance on AI makes it imperative to discuss the future implications of adopting AI systems in diagnostic medicine, as well as the challenges that accompany this shift.

Diagnostic applications of AI rely on training models with vast amounts of medical data and imaging, which contribute to improving diagnostic precision and accelerating the detection of diseases. However, these benefits also necessitate proactive legal and ethical oversight to safeguard human rights from potential harms linked to these emerging technologies.

Thus, growing academic and professional interest is being directed toward identifying the legal liabilities that may arise from the use of AI in healthcare, particularly in terms of establishing responsibility for errors

or harm caused by such systems. This underscores the importance of the present study, which aims to clarify these issues and contribute to the ongoing legal discourse.

Significance of the Study

The importance of this study lies in its exploration of the legal foundations of liability arising from damages caused by the use of technological tools and AI in the medical sector. It seeks to identify potential solutions and safeguards that protect human rights while assessing the adequacy and effectiveness of existing legal rules concerning both medical and technological liability.

Objectives of the Study

This study aims to:

– Provide a comprehensive overview of the legal basis for liability resulting from the use of modern technologies in the healthcare sector.
– Assess the sufficiency of current legal frameworks in providing effective protection for individuals against risks associated with these technologies.
– Explore potential legal and regulatory solutions to mitigate harm and enhance protection in the use of modern healthcare technologies.

The Concept of Artificial Intelligence in the Healthcare Sector

Artificial Intelligence (AI) refers to software systems—and potentially hardware systems—designed by

umans to perform complex tasks in real or digital environments. These systems operate by perceiving their surroundings, acquiring information, interpreting structured or unstructured data, and applying analytical processes to knowledge or data-derived insights to determine the most appropriate action to achieve a specific goal. AI can utilize symbolic rules or learn from digital models, and may also adapt its behavior based on analysis of how its previous actions influenced the environment[i].

In the medical context, AI broadly denotes the use of machine learning algorithms to simulate human cognitive processes in analyzing complex medical and health-related data. This enables the interpretation, presentation, and understanding of such data with greater sophistication. Compared to traditional healthcare technologies, AI is distinguished by its ability to collect, process, and deliver clear and actionable results to end users.

II. The Ethical and Legal Framework for AI in the Healthcare Sector

It is essential that the use of AI in healthcare adheres to an ethical and legal framework that safeguards the rights and interests of all stakeholders involved. In this regard, the World Health Organization (WHO) outlines six core principles that should guide the design and deployment of AI in the health sector[ii]:

1. **Protecting Human Well-being:**

The primary aim of AI in healthcare must be to enhance the health and well-being of all individuals and communities, without discrimination or marginalization.

2. **Promoting Solidarity:**

AI should contribute to reducing health disparities and improving equity among patients and healthcare workers at local, regional, and global levels[iii].

3. **Respecting Individual Rights:**

AI applications in healthcare must respect the rights, freedoms, and privacy of individuals, without infringing on their autonomy, decision-making, or will.

4. **Ensuring Transparency:'**

The development, deployment, and utilization of AI in healthcare must be transparent, interpretable, and verifiable, enabling individuals and communities to understand how decisions are made and how these impact their live[iv]s.

5. **Fostering Responsibility:**

All parties involved in the creation, dissemination, and application of AI in healthcare must bear legal and ethical responsibility for its outcomes—whether beneficial or harmful.

6. **Guaranteeing Accountability:**

Effective mechanisms must be in place to ensure accountability at all levels, enabling individuals and groups to seek and obtain fair compensation in the event of harm or adverse effects resulting from AI use in healthcare[v].

III. Recognizing the Legal Personality of Artificial Intelligence

The legal system fundamentally distinguishes between "persons" and "things," assigning distinct legal rules to each category based on their inherent nature and anticipated roles. Legal personality is what qualifies an entity to actively participate in legal relationships, thereby making legal persons the sole subjects capable of initiating and bearing legal obligations. In contrast, "things" are merely the objects of legal relationships, assigned a purely utilitarian status.

Legal personality enables its holder to act as a legal subject, capable of entering into relationships with other persons to fulfill specific legal purposes. This aligns with the role of law as a tool for organizing social behavior. Historically, this status was exclusive to human beings, contingent upon meeting specific criteria. Over time, however, legal personality has been extended to non-human entities—such as corporate bodies and institutions—that lack biological life or intelligence[vi].

Emerging discussions now advocate for further expanding the notion of legal personality to include entities that either share biological traits with humans (such as animals and elements of nature) or, in the case of artificial intelligence, exhibit cognitive capabilities comparable to human intelligence. Since the law has already granted legal personality to juridical persons that neither possess biological life nor intelligence, it is argued that granting such status to AI systems—especially those performing autonomous actions—should be even more justifiable. This would serve as a mechanism for assigning civil liability for actions committed by these technologies, and provide the necessary legal framework for protecting both the public and the technology itself[vii].

Granting legal personality to intelligent robots has been proposed as a way to limit the liability of their owners and operators. However, this legal construct does not fully align with traditional legal standards for personhood, as it tends to overestimate the actual capabilities of robots. Moreover, equating intelligent robots with natural persons raises serious concerns. If robots were to be granted full legal personality, they would also be entitled to fundamental human rights—such as dignity and citizenship—which would conflict with core principles of international human rights law, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights[viii].

Equally, extending legal personality to AI in the same way as to corporate entities is problematic. Legal persons are governed and represented by natural persons who are ultimately accountable for their actions—something that does not apply to autonomous AI systems. Recognizing AI as a legal person could therefore serve to shield developers, manufacturers, and users from liability, creating a significant gap in accountability.

Some legal scholars argue that natural legal personality is granted to the human body regardless of its cognitive abilities, which raises a complex issue when applied to AI. Nonetheless, the link between legal personality and legal responsibility remains crucial. Establishing clear accountability for AI's actions requires a nuanced legal framework—one that does not merely assign personality, but ensures ethical responsibility and legal oversight.

A person lacking mental capacity may still enjoy legal personality and possess an independent legal patrimony, despite being exempt from personal liability. This does not imply absolute immunity from

liability; rather, the burden of liability is transferred to the responsible party, who may then be required to provide compensation[ix].

From this perspective, granting legal personality to artificial intelligence in a manner equivalent to that of natural persons constitutes an encroachment on human rights. The attribution of rights and obligations is what defines legal personality, and AI cannot be granted this status in the same way as a juridical person either, since legal persons possess independent patrimony and are administered by natural persons[x].

However, in light of the significant advancements in intelligent robotics—which now simulate human behavior—there is a growing need to reconsider the issue. The purpose of assigning legal personality to AI is not to grant it full human rights, but rather to establish a clear mechanism for identifying the party responsible for any harm caused. AI entities are often the product of collaborative input from multiple parties, such as developers, manufacturers, and operators. In cases of damage or harm, victims are left to search for the liable party. This highlights the importance of treating AI systems as legal entities subject to accountability, similar to corporations, in order to strengthen the legal system's ability to address the novel challenges posed by AI. This step would ensure the law keeps pace with technological change and enhances human–AI interaction[xi].

A relevant precedent is found in the case of In Klein v. U.S., where a pilot activated the autopilot during landing, contrary to aviation regulations that prohibit its use in such a situation. The plane sustained severe damage due to a poor landing executed by the autopilot. While the autopilot technically committed the error, liability ultimately rested with the pilot, who was responsible for its misuse[xii].

This example underlines that the goal of recognizing legal personality in AI is to establish a clear framework of responsibility for damages caused by autonomous systems. While the recognition of rights protects AI from abuse, the imposition of duties ensures others are protected from the consequences of AI's actions.

IV. Challenges of Using Artificial Intelligence in the Healthcare Sector

Despite the considerable benefits AI brings to healthcare, its growing use in medical diagnostics and patient care—from its early stages to more advanced applications—has raised a number of significant challenges, including:

- **Balancing Privacy with Technological Advancement:**

This is especially complex in healthcare, where patient data is a crucial component for developing AI algorithms. However, such data is highly sensitive, making it challenging to expand AI applications while preserving patient privacy.

- **Bias Arising from Data Diversity:**

Ensuring high-quality, representative data is essential for producing accurate and unbiased AI outcomes. Current datasets often focus on specific demographic groups, potentially excluding underrepresented populations, which can compromise fairness and effectiveness[xiii].

- **Integration with Legacy Systems:**

Many healthcare institutions face limitations in digital infrastructure, hindering the implementation and integration of AI solutions into existing systems. This impedes the full realization of AI's potential in clinical environments.

- **Weak Regulatory and Ethical Guidelines:**

The absence or insufficiency of robust legal frameworks governing AI use in healthcare creates uncertainty. Rapid advancements in AI outpace current regulations, raising concerns about data privacy, informed consent, and responsible use[xiv].

- **Lack of Transparency in Decision-Making:**

The so-called "black box" nature of AI algorithms makes it difficult to explain how decisions—such as diagnoses—are made. This lack of interpretability can erode trust among patients and medical professionals, and hinder the broader adoption of AI technologies[xv].

- **Technical Vulnerabilities:**

The potential for system failures remains a serious concern. As healthcare providers increasingly rely on intelligent systems, technical malfunctions could disrupt care and, in critical cases, pose severe risks to patient safety[xvi].

V. Legal and Ethical Challenges of Using Robots in the Healthcare Sector

Robot ethics concern the moral dilemmas that arise in the development and deployment of robotic systems—particularly when robots are introduced into sensitive areas such as healthcare. Medical robots, in particular, present a distinct set of ethical and legal challenges. Key areas of concern include[xvii]:

1. **Patient Safety and Liability:**

As medical robots become more involved in patient care, ensuring their safety and reliability becomes essential. Any malfunction or error in robotic performance can lead to serious consequences, including patient injury or death. Determining liability in such cases is complex, as it may involve multiple actors—such as manufacturers, programmers, operators, and healthcare providers.

2. **Informed Consent and Decision-Making:**

Medical robots are often used in critical procedures, including surgeries. In such contexts, the principle of informed consent is vital. Patients must be adequately informed about the robot's capabilities, limitations, and potential risks in order to make autonomous and informed decisions regarding their treatment. Ensuring patient involvement in decision-making processes involving robotic systems is a key ethical consideration.

3. **Data Privacy and Security:**

Medical robots and associated systems collect and process vast volumes of sensitive patient data, including personal health records, medical histories, and other confidential information. Safeguarding the privacy and security of this data is essential to maintaining patient trust and ensuring compliance with legal frameworks, such as the Health Insurance Portability and Accountability[xviii] Act (HIPAA).

4. **Equitable Access and Affordability:**

The integration of robotic technology into healthcare may lead to increased costs. Ensuring equitable access to medical robotics and addressing disparities in their availability is critical. Consideration must also be given to affordability to prevent such technologies from becoming accessible only to privileged segments of society.

5. **Autonomy and Clinical Decision-Making:**

The increasing autonomy of medical robots raises important questions about the evolving role of healthcare professionals and the nature of the physician–patient relationship. Decisions made by robots that directly impact patient care must remain transparent and subject to oversight by qualified medical personnel. Maintaining human oversight and accountability is crucial in preserving ethical and legal standards in clinical practice.

VI. Artificial Intelligence and Legal Liability

A central question arises: to what extent can legal liability—whether civil or criminal—be assigned for actions committed by artificial intelligence (AI), particularly in the medical field? This is especially relevant for AI diagnostic support systems, which have demonstrated exceptional capabilities in performing complex tasks such as data analysis and decision-making assistance. These advancements have prompted a reconsideration of traditional liability rules, introducing new and distinct legal dimensions.

1. Criminal Liability for the Use of AI in Healthcare

Harm to human health is a real possibility in scenarios where robots are involved in patient care. Since robots are not natural persons, liability for crimes committed by such systems is typically determined in a manner analogous to that used for corporations—by identifying the natural person who is legally responsible or who benefits from the robot's actions[xix].

In jurisdictions such as India and many other countries, robots have not yet been granted legal personality. Given their capacity to act autonomously, one proposal is to create commercial entities specifically to operate autonomous agents such as software and robots, thereby allowing responsibility to be clearly assigned[xx].

Legal scholar Gabriel Hallevy has proposed three models of criminal liability applicable to AI systems:

A. Model 1: Perpetration via Another (Operator or User Responsibility)

This model is based on the assumption that AI lacks human characteristics and, therefore, cannot be considered a perpetrator of a crime. It treats AI systems similarly to individuals with limited mental capacity—such as children or those deemed legally incompetent—who cannot possess criminal intent (*mens rea*). Here, AI is viewed as an "innocent agent" or tool, used by a human perpetrator who is the true mastermind behind the criminal act.

Thus, liability lies with the individual who operated, programmed, or misused the AI system. The requisite criminal intent is attributed to the mental state of the human actor who directed the AI's behavior.

B. Model 2: Natural and Probable Consequence Liability

This model holds that even if the programmer or user did not intend to commit a crime, they may still be held responsible if the crime was a foreseeable and probable outcome of using the AI system.

Even in the absence of knowledge or intent to commit a crime, if evidence shows that the programmer or user *should have foreseen* the AI's potentially harmful behavior and failed to prevent it, they may be prosecuted. This approach does not require intent but relies on negligence, emphasizing the lack of due diligence in deploying AI that could foreseeably result in unlawful acts[xxi].

C. Model 3: Direct Liability Model

This model provides a theoretical framework that places AI entities on par with humans for purposes of criminal liability, assuming they meet the two basic conditions of criminal law:

- **Actus reus** (the criminal act)
- **Mens rea** (criminal intent)

If an AI system can satisfy both conditions, it could be held directly criminally liable. Implementing this model requires granting legal personality to AI entities. A symbolic step in this direction was taken by Saudi Arabia, which granted legal status to the humanoid robot Sophia in 2017.

Hallevy argues that this model may become essential as countries begin to recognize robots as legal persons. When this happens, AI systems could be treated as independent entities capable of being prosecuted, especially when they make autonomous decisions and act without direct human input[xxii].

2. Civil Liability for the Use of Artificial Intelligence in the Medical Field

A logical and pressing issue concerns compensation for harm caused by artificial intelligence in healthcare, particularly under civil liability frameworks. In this regard, two main legal systems are commonly referenced:

- The **liability for things** (*responsabilité du fait des choses*), and
- The **liability for defective products** (*responsabilité du fait des produits défectueux*).

A. Liability for Things

Some legal scholars argue that the general rules of civil liability for things are sufficiently flexible to encompass damages caused by AI in the medical field. Under this theory, a "guardian" (*gardien*) is defined as the individual who exercises effective control over an object—particularly the power to use, direct, and supervise its functioning. It is essential to note that being the guardian of a thing does not necessarily mean being its owner; legal guardianship and ownership are distinct concepts.

For liability to be engaged under this framework, the damage must be the result of the object's autonomous actions while under the guardian's control. This constitutes strict liability, which does not require proof of fault but is instead based on presumed fault or, more precisely, risk-based liability. For example, if a medical robot causes harm to a patient, the person exercising control over the robot would bear the risk associated with its use, whether that person is the owner, operator, or another party with actual authority over it[xxiii].

Given that medical AI encompasses a wide range of applications—some integrated into physical devices (e.g., surgical robots)—the AI system may be embodied in a physical form. In cases where such integrated AI is involved in surgery and causes harm, responsibility would lie with the guardian of the robot. This could include the physician performing the operation, the hospital owner, the robot's manufacturer or developer, or any party who exercises effective control over the robot equipped with AI[xxiv].

Opposing View: Inapplicability of "Thing-Based" Liability to Medical AI

However, a significant portion of legal scholarship rejects applying this regime to AI in healthcare for several reasons:

• AI Is Not a Physical Object

The regime of liability for things was designed for inanimate, physical objects that lack autonomy. It presupposes a one-directional relationship in which humans control machines. However, modern AI technologies—particularly autonomous medical systems—are increasingly self-operating and capable of learning and adapting beyond human control[xxv].

Many scholars therefore argue that AI cannot reasonably be considered a "thing" in the traditional sense. As a digital, intelligent entity capable of acquiring skills and acting independently, AI defies the boundaries of simple objecthood. Consequently, classifying such a system as a mere "thing" under the law would be reductive, if not entirely inadequate.

• Difficulty in Identifying the Responsible Guardian

In theory, a guardian is the person who has the effective power to use, direct, and supervise an object. However, determining who holds this power over an AI system—especially one embedded in a robotic device—is not straightforward. The core issue is identifying who truly possesses control power (*le pouvoir de contrôle*) over the AI.

Is it the owner of the AI system (e.g., the hospital or healthcare institution)? Or is it the user (e.g., the treating physician), who makes the operational decisions and chooses whether or not to use a particular AI-powered tool for a specific patient?

In practical terms, physicians often have actual decision-making power over the use of AI applications in treatment. Therefore, under this model, if a patient suffers harm as a result of the robot's actions, the physician could be deemed the guardian and held liable, meaning they would be responsible for compensating the patient for damages[xxvi].

B. Liability for Defective Products

Liability for defective products is a form of strict liability that does not require proof of fault. The European legislator established its rules in **Directive 85/374** of **25 July 1985**, aimed at addressing shortcomings in national liability laws within European legal systems, which had previously failed to offer adequate protection for consumers in cases where purchased products were found to be defective. As such, assigning

liability to the manufacturer or producer was justified by the increasing complexity of modern technology and the need to attribute the risks inherent in advanced production to those introducing it to the market[xxvii].

Article 1 of Directive 85/374 clearly states that the **producer shall be liable for damage caused by a defective product**.

Some legal scholars argue that the rules of defective product liability are more appropriate for addressing harm caused by **artificial intelligence**, particularly in the medical field, than traditional liability for things. There is no doubt that AI in healthcare constitutes an advanced technology that inevitably introduces new risks into society. A defective product, in this context, may be a software application that fails to meet legally expected safety standards, resulting in harm. In such cases, liability falls upon the party responsible for introducing and marketing the defective technology—namely, the manufacturer[xxviii].

Conclusion

Advancements in artificial intelligence may soon enable robots to independently perform laboratory tests, remove arterial plaque, extract tissue biopsies, and target cancerous tumors. In the near future, robots may also administer precision medications, manage routine patient care, and engage in preliminary consultations regarding symptoms.

Undoubtedly, technology will play a vital role in the evolution of healthcare, and AI will be an integral part of this transformation. However, before such widespread integration occurs, there is a pressing need for a comprehensive legal and regulatory framework to govern the operation of robots in healthcare, ensuring that they are deployed in safe, ethical, and controlled ways.

Currently, many Arab legal systems lack specific legislation governing the use of robots and AI in general, and particularly in the medical field. This legislative gap highlights the importance of continued research in legal scholarship to keep pace with developments in robotics and AI—especially their legal dimensions. Such efforts are crucial for forming informed legal perspectives that contribute to the drafting of regulations and guiding principles for the responsible use of medical robotics.

References :

1. [i] [i]Commission européenne .lignes directrices en matière d'éthique pour une intelligence artificielle digne de confiance ,08 avril 2019 ,p09 et 143.
2. [ii] M. Cascella, Laura. "Artificial Intelligence in Healthcare: Challenges and Risks.
3. [iii] Ahmed Ibrahim, Legal Liability Resulting from Artificial Intelligence Errors in UAE Law, PhD thesis, Ain Shams University, 2020
4. [iv] Al shawwa SZ, Kassem AA, Farid RM, Mostafa SK,Labib GS.Nanocarrier Drug Delivery Systems:Characterization, Limitations, Future Perspectives and Implementation of Artificial Intelligence.Pharmaceutics.2022 Apr 18; 14 (4): 883.
5. [v] Ahmed Shawqi Omar, Criminal Law and Modern Medicine, Dar Al-Nahda Al-Gharbiyya, Cairo, 2007.
6. [vi] Roberto Andorno la distinction juridique entre les personnes et les choses a lépreuve des procréations artificielles,L ,G ,D,J paris 1996, p 62
7. [vii] A. Hendoza – caminade , le droit confronte a l intelligence artificielle des robos m vers lémergence de nouveaux concepts juridiques ? D 2016 ,p 445 .
8. [viii] Bertsia, "Legal liability of artificial intelligence driven-systems (AI)", master thesis, international hellenic university, 2019
9. [ix] Oliveira, "La responsabilité civile dans les cas de dommages causés par les robots d'assistance au Québec", LL.M, faculté de droit, université de montréal, 2016
10. [x] Abbott, The reasonable robot. Cambridge University Press: University of Surrey School of Law, 2020

11. [xi] Assunta Cappeli, “regulation on safety and civil liability of intelligent autonomous robots: the case of smart cars”, Ph. D thesis, universita degli studidi Trento, 2014.
12. [xii] Benhamou and J. Ferland, Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages, submitted to as a book chapter: Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law, P. D’Agostino, , et al., 2020
13. [xiiixiii] Ahuja, Abhimanyu S. “The impact of artificial intelligence in medicine on the future role of the physician.” PeerJ vol. 7, Oct. 2019, p. e7702
14. [xiv] Collier, Matthew, and Richard Fu. “Artificial Intelligence in Healthcare.” Accenture 30 July 2020
15. [xv xv] W. Nicholson Price. “Risks and Remedies for Artificial Intelligence in Health Care.” Brookings, 14 Nov. 201
16. [xvi xvi] The Importance of Artificial Intelligence (AI) in Improving Diagnostics and Treatments.” Acelera Pyme, 6 Oct. 2023
17. [xvii] https://iamaeg.net/ar/publications/articles/legal-aspects-of-medical-robots
18. [xviii] calo, R. (2012). Robots and Privacy. In P. Lin, G. Bekey, & K. Abney (Eds.), Robot Ethics:
19. [xix] Das KP, J C. Nano particles and convergence of artificial intelligence for targeted drug delivery forcancer therapy: Current progress and challenges. Front Med Technol.2023 Jan 6; 4: 1067144.
20. [xx] The Ethical and Social Implications of Robotics (1st ed., pp. 187-202). Cambridge, MA:MIT Press
21. [xxi] felzmann, H., Beyan, T., Ryan, M., & Beyan, O. (2015). Implementing an ethical approach to big data analytics in assistive robotics for elderly with dementia
22. [xxii] Schweikard, Achim & Ernst, Floris (October 2015). Medical Robotics. Springer Science -Business Media. doi:10.1007/978-3-319-22891-4. ISBN 978-3-319-22890-7. S2CID 32424869
23. [xxiii] Mohamed Labib Shanab, Liability for Acts of Things: A Study in Egyptian and French Law, 1st Edition, Dar Al-Thaqafa for Publishing and Distribution, p. 63.
24. [xxiv] Abdullah Saeed Abdullah Al-Wali, Civil Liability for Damages: Applications of Artificial Intelligence in UAE Law – A Comparative Analytical Study, Dar Al-Nahda Al-Arabia, Egypt, 2021, p. 273.
25. [xxv] P. Brun, La responsabilité du fait des objets connectés, Lamy Droit de la Responsabilité, 2018, Nos. 350–60.
26. [xxvi] Talal Hussein Ali Al-Roud, Civil Liability for Damages Caused by Artificial Intelligence-Based Technology Operators: A Comparative Study, PhD Dissertation, Faculty of Law, Mansoura University, Egypt, 2022.
27. [xxvii] Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products.
28. [xxviii] Mohamed Mohamed Abdel Latif, Liability for Artificial Intelligence Between Private and Public Law, paper presented at the 33rd Conference on the Legal and Economic Aspects of Artificial Intelligence and Information Technology, Faculty of Law, Mansoura University, Egypt, 24 May 2021.