

The Steady Development of Digital Law: New Challenges of Artificial Intelligence

Tareck ALSAMARA¹, Farouk GHAZI²

Abstract

The article addresses the issue of the steady development of digital law in the face of artificial intelligence (AI) technology. Some international institutions are focusing on the potentially dangerous aspects of artificial intelligence. In March 2024, the first legal text from the European Union relating to artificial intelligence was issued. The rules of digital law pertaining to artificial intelligence are spread across all branches of law, and both international and national laws contribute to the continuous development of this field. The article uses a deductive approach by showing how international law and national law have contributed to the development of digital laws to accommodate artificial intelligence technology. The article concludes that such laws have effects on other branches of law, and can help to find solutions to the problems of using artificial intelligence. Similarly, we seek to find solutions to problems in other areas such as civil and commercial law. Such laws as the Personal Data Protection Law, the rules of the Consumer Protection Law, and the Copyright Protection Law that apply to digital content play an important role in preventing abuses. Such protections are also needed in the field of AI.

Keywords: *Digital Law, Artificial Intelligence, Data Protection, Cyber Crime, Digital Consumer Protection, European Union.*

Introduction

Artificial intelligence is based on making machines as intelligent as a human beings, by making them capable of self-learning. The world is witnessing an increasing interest in artificial intelligence systems, as legislative care for the digital field has evolved from classical rules to more advanced rules, and digital technology has a significant presence in daily life. Naturally this includes the field of commerce (Meltzer, 2019; Dhali 2022), as commerce has evolved from e-commerce to digital commerce (Janow & Mavroidis, 2019). Even the management of public facilities in all countries of the world has become digital, due to the many financial benefits provided by digital services (Schrock, 2019). The current time is witnessing the availability of this technology to all segments of society. This has resulted in all branches of law becoming concerned with regulating the digital nature of the activities to which they are subject. For example, civil law regulates digital contracts and electronic signatures; commercial law regulates digital trade activities (Novruzova et al, 2020); and penal law deals with crimes of a digital nature such as cybercrimes (Ruddin, 2024). Intellectual property protection law also deals with digital content, providing guarantees related to the moral rights of its owners (Margono, 2024). Accordingly, digital law can be defined through a comprehensive and multidisciplinary approach, i.e. a definition that includes all the branches of law mentioned. Digital law can also be defined as a set of legal rules that regulate the digital domain. These rules are widespread among the branches of law.

Related Work

We should refer to Surden's article titled : "Artificial intelligence and law: An overview." In it the author aimed to clarify the relationship between artificial intelligence and law. AI currently lacks the ability to be conscious or intelligent in the human sense. Today's AI technology uses patterns, rules, and heuristics to make beneficial decisions in specific settings, without requiring input. However, existing AI technology has some limits. It struggles with abstract concepts, comprehension, knowledge transmission, and unstructured or open-ended work. AI has been successful at highly organized tasks, such as chess, credit card fraud, and tumor detection, all areas requiring obviously correct or incorrect replies (Surden, 2019). The Akpuokwe et al article offered an excellent overview of the complicated legal issues raised by the spread of artificial

¹ Assistant professor, Prince Sultan University, Kingdom Saudi Arabia.

² Associate professor, Annaba Badji Mokhtar University, Algeria, Email: ghazifarouk1@gmail.com.

intelligence (AI) and robots. This comprehensive examination covers the many features of the emerging legal landscape, focusing on concerns at the interface of technology and law. Key focus points include autonomous AI system liability frameworks, ethical considerations in intelligent machine deployment, and the complicated dynamics of data privacy in the age of pervasive automation. The assessment digs into the complicated legal complexities of intellectual property rights, with a focus on how AI systems contribute to creative outcomes and innovation. It navigates the hazy lines between human and computer creation, posing fundamental questions about ownership and protection in the digital era. Furthermore, the study emphasizes the global dimension of these difficulties, and emphasizes the need for international cooperation to develop unified legal standards. As AI and robotics transform sectors and societal frameworks, the analysis emphasizes the crucial importance of adaptive and anticipatory legal frameworks. It investigated how existing legal paradigms are dealing with the tremendous speed of technological advancement and describes the ethical quandaries that arise from outsourcing decision-making to intelligent algorithms (Akpuokwe et al, 2024). The Igbinenikaro and Adewusi paper aimed to close a gap by investigating the distinct legal issues provided by AI in the context of international trade agreements. Their study started with a review of the current state of AI technologies and their applications in global trade. Then it examined the existing legal frameworks in international trade agreements to find areas of uncertainty and inconsistency regarding AI. The study looked at case studies and examples of AI deployment in trade, as well as the legal consequences and issues that may arise. Finally, the study made recommendations and policy guidelines for incorporating AI into future trade agreements while maintaining coherence, justice, and adaptability in the face of ever-changing technological advancement.

Methodology

The article uses a scientific methodology based on several approaches. First is the comparative approach, which makes a comparison between branches of law in order to extract the legal provisions that apply to artificial intelligence. Next, the descriptive approach used to describe laws and legal systems. This is done through two basic stages: the first is identifying the challenges raised by artificial intelligence, and the second is identifying the legal frameworks closest to addressing these challenges.

Results And Discussion

Applicable Law On Ai

Artificial Intelligence Systems and Personal Data Protection Laws

Personal data protection laws play an important role in the digital field (Smirnova & Travieso-Morales, 2024; Hassan, 2021), and these laws apply to artificial intelligence systems, as these laws protect the privacy of individuals and protect their personal data (Bakare et al, 2024). Such personal data as name, surname and photo represent important material for commercial companies in the digital field, and personal data laws have imposed a set of controls on those who process this data. For example, Article 5 of the European Personal Data Protection Law represented by European Union Regulation No. (2016/679) was issued by the European Parliament and the Council on April 27, 2016. It deals with the protection of individuals with regard to the processing of personal data and the freedom of access to this data. Article 5 states that data must be processed according to a set of principles, which are (Joyce & Javidroozi, 2024): (1) legitimacy, loyalty and transparency, meaning not relying on misleading means; (2) the principle of data minimization, which means not requesting unnecessary data; (3) the principle of data accuracy; (4) the principle of time limitation for retention (Calvi, 2024). It is important to note that the law is binding on every company operating in the European Union, and even on companies not located in the European Union but providing services and products to citizens located in the European Union (Sarabdeen & Mohamed Ishak, 2024; Farouk & Alsamara, 2023).

Artificial Intelligence Systems and Consumer Protection Laws

Consumer protection laws also play a leading role in the field of artificial intelligence software activities. Laws such as the California Consumer Privacy Act apply to the digital consumer (Pardau, 2018), and personal information is defined more broadly to include any information that identifies, relates to, describes, or can be linked to a consumer, including categories such as browsing history, geolocation data, and inferences drawn from any personal information to create a consumer profile (Harding et al, 2019). Consumers have rights such as the right to know what personal data is being collected (Bakare et al, 2024), the right to delete personal data (Harisson, 2022), the right to opt out of the sale of personal data, and the right to non-discrimination in exercising their privacy rights (Baik, 2020).

Artificial Intelligence Systems and Intellectual Property Laws

Intellectual property laws are of utmost importance in digital law (Vargas & Torres, 2024). They protect digital content by dedicating exclusive rights to the owner of the digital content, as he has the exclusive right to print, publish, display, and other rights. These rights are exclusive, meaning that the owner alone enjoys them, and only the owner of these rights can transfer them to others by selling them or licensing their exploitation. To activate the protection of these rights, some laws require the registration of the content, while legislation in Europe and the United States does not require registration, as they have adopted the principle of automatic protection (Widla, 2024). Currently, there is a great deal of debate about intellectual property related to the contents generated by artificial intelligence applications (Gaffar & Albarashdi, 2024). The efforts of international law and national legal texts of countries overlap to provide significant protection for copyrights (Albakjaji & Almarzouqi, 2024). It is important to point out the Berne Convention, as the Berne Convention, adopted in 1886, deals with the protection of works and the rights of their authors. The agreement allows creators, such as authors, musicians, poets, painters, etc., to control how their works are used, by whom, and under what conditions (Schow, 2023). Anyone whose intellectual and copyright rights are affected by digital content can ask the courts to compensate them or to request a halt to ongoing violations of their intellectual property rights (Sung, 2020). Arbitration also plays a major role in settling disputes between individuals in the field of digital content (Bakhramova, 2024; Alsamara & Ghazi, 2024). The Digital Millennium Copyright Act in the United States is considered the most comprehensive law dedicated to digital content (Lunney, 2001).

Artificial Intelligence Systems and Criminal Laws

Software piracy is a subject in which all branches of law intervene (Koen Jr & Im, 1997). It involves the civil liability of the person who caused it. It also involves civil tort liability. This is a form of civil liability that aims to compensate victims of damage caused by a person to another person without there being a contract. The origin of this idea goes back to Roman law, which distinguished between civil and criminal wrong. In France, tort liability was enshrined in the Civil Code of 1804. It was then developed through case law and underwent a major development under the Law of July 5, 1985 on traffic accidents, which established a system of liability for traffic accidents. This area of civil law requires the necessity of compensating the injured party for the act of digital piracy (Straub Jr & Collins, 1990). Criminal law also intervenes by considering piracy as an act that constitutes a crime, as criminal liability relates to the responsibility of a person towards society for acts that are considered by law to be crimes of a criminal nature such as theft, murder or physical assault. Such liabilities are subject to the rules of criminal law. The purpose of criminal liability is to punish illegal behavior and deter others from committing similar acts. Tort liability relates to harm to a person or his property, while criminal liability relates to violations of criminal law and behaviors that are considered harmful to society as a whole. It is important to note that acts that give rise to civil liability may also constitute a criminal offense. For example, if a person intentionally causes harm to another, he may be held liable for this harm at both the civil and criminal levels. The two types of liability are dealt with separately and are governed by separate legal rules, as the penal laws of countries establish penalties for the crime of software piracy (Rahman & Pandey, 2020). International law is also establishing means of international cooperation to confront this transnational crime (Asongu, 2018). The Computer Fraud and Abuse Act (CFAA) is the most important classic rule that has emerged, and it is a US federal law that criminalizes various activities related to computer fraud and abuse (Simmons, 2016). It addresses a wide range of behaviors that involve unauthorized access to computer systems and the misuse of information obtained from this access (Chung, 2010). There are several acts that constitute a cybercrime

(Goldman, 2012). National legislations of countries mention them in detail, and they constitute the material element of cybercrime. The material element of cybercrime represents the greatest challenge to laws, because the continuous technological development makes it difficult for laws to keep up with all the new developments in the field of cybercrime.

Generative artificial intelligence through texts, images, etc. must also respect the rules of international law in preventing hate speech, because this enhances the status of human rights and dignity. It is known that almost all countries' legislation prohibits hate speech (Lepoutre et al, 2024), as hate speech is what constitutes a discriminatory practice based on race, color or language and causes harm to individuals (Carlson & Terry, 2024). There is a current trend towards using artificial intelligence in the field of processing hate speech, due to its high capacity in the field of collecting and detecting this type of speech in the digital space (Cortiz & Zubiaga, 2020).

The Future of Digital Law in the Age of Artificial Intelligence

Currently, there are no specialized legal texts for liability for artificial intelligence, but civil law can provide a temporary framework for courts to settle disputes related to the uses of artificial intelligence.

Liability For Artificial Intelligence Devices as A Defective Product

European legislation has produced one of the most recent legislations in this field, Directive No. 85/374. This directive, adopted in 1985, established the basic principles of liability for defective products in the European Union. Based on it, manufacturers are required to compensate victims of defective products without the need to prove fault (Navas, 2020). In order for the manufacturer to be liable, three conditions must be met: first, the product must be defective, second, the damage must have occurred, and third, there must be a causal relationship between the defective product and the damage (Wuyts, 2014). However, the legal text does not specifically refer to artificial intelligence systems, but it provides a framework that includes all products, and so may be extended to AI (Buiten, 2024).

Liability For Damages Caused by Artificial Intelligence Systems

It must be noted that responsibility is only borne by those who have legal personality. Therefore, before discussing the question of whether artificial intelligence systems can be held liable for the damages they cause, the question must be asked: Do artificial intelligence systems have legal personality according to current international and national laws? The apparent truth is that in legal systems, legal personality is divided into a natural legal personality (exclusively human) and a moral legal personality (for public and private institutions) (Solum, 2020). Moral personality refers to the legal capacity of an organization such as a company, association, private institution, or public institution to obtain rights and obligations and to be a party to contracts and to initiate legal proceedings. Unlike natural persons who have legal personality by virtue of their physical existence, legal persons acquire their legal personality through legal recognition or legal creation. This allows them to operate as separate entities with their own assets, liabilities, and obligations. Legal personality is of particular importance because it allows an organization to carry out business activities and bear legal responsibilities without directly involving the natural persons who compose it. Currently, AI systems and devices do not have the status of legal person (Chesterman, 2020). AI systems do not have a financial liability to be subject to fines, confiscations, and judicial compensation orders. The person who exercises effective control over AI systems remains liable for the damages they cause, even if these systems are autonomous and self-operating. Civil law represents the framework closest to covering this civil liability (Durneva et al, 2021). For example, in France, article 1242 of the Civil Code currently constitutes a fundamental pillar in the field of civil liability related to such things. However, within the framework of this article, special circumstances emerge that determine the cases in which its application is restricted by specific regulations. These regulations, which were created to better respond to the specificities of each case, define the categories of things and the circumstances covered by different articles (Lee, 2024). Article 1242 of the French Civil Code explicitly states: "We are responsible not only for the damage we cause through our actions, but also for the damage caused by the actions of persons for whom we must answer, or by things in our custody." The importance of the topic is emerging at the present time

after the increasing use of artificial intelligence systems in the medical field, as they are used independently in the field of medical diagnosis and treatment. This calls for an ethical and legal debate (Schneeberger et al, 2020). The topic has been discussed by medical unions, and medical law remains the outlet for determining doctors' responsibilities for the errors of intelligent machines (Naik et al, 2022). At the European level, there is interest in the topic from the European Council and the European Union. At the level of the European Council, the Committee of Ministers adopted a recommendation on April 8, 2020 regarding the impact of algorithmic systems on human rights, as the recommendation stressed that the member states of the European Council have a responsibility not to violate human rights by algorithmic systems (Elkadi, 2021). The obligations of states revolve around enacting legislation and developing national policies in partnership with stakeholders, raising awareness among individuals about the ability of algorithmic systems to threaten human rights, and establishing national institutions in each country whose mission is to ensure that human rights are not violated by algorithmic systems.

At its plenary session on June 18, 2020, the European Parliament formed the Special Committee on Artificial Intelligence in the Digital Age (AIDA) with the goal of developing a long-term EU strategy for artificial intelligence (AI). Building on the Standing Committee's earlier findings, the Committee will assess the impact and challenges of AI implementation, identify common EU objectives, and make recommendations on the best path ahead. Over the next 12 months, the Commission intends to take a horizontal approach to AI, investigating its potential influence on the EU economy with a focus on skills, employment, education, health, transportation, the environment, industry, e-government, and transnational collaborations. To meet its objectives, the Committee members have organized hearings and workshops with key stakeholders such as experts, policymakers and entrepreneurs. In France, the Leading Committee on Digital Ethics, overseen by the National Advisory Commission on Ethics, is responsible for providing opinions on the referrals entrusted to it, informing public discourse on digital ethics concerns, and formulating ideas for sustaining digital ethics. It also contributes to national reflection on digital ethics. Created in December 2019, at the request of the French Prime Minister, it is supervised by the National Advisory Committee on Ethics. In the field of the use of artificial intelligence in health, the committee made recommendations centered on the need to continue teaching existing diagnostic methods, which do not include AI systems used in medical diagnosis previously, and to be the subject of research aimed at developing them. The growing place of AI systems used in medical diagnosis in the field of medical skills also requires in-depth studies on the interaction between humans and AI technologies to assess the impact of AI systems used in medical diagnosis in the practice of medicine. For the sake of transparency and traceability, the use of AI systems used in medical diagnosis must be indicated in the medical report of the consultation. These elements converge in favor of human control at all stages of care, from the consultation to the examinations and the results of the analyses and the interpretation of these results.

Conclusion

Artificial intelligence is a useful reality for the legal field, as it helps in analyzing big data and contributes to the technical treatment of some digital diseases such as hate speech and racial discrimination in digital social media. The efforts of both the European Union and the European Council represent a clear indication of Europe's desire to establish a legal framework for artificial intelligence systems, and these initiatives are absent in other parts of the world. For example, there are no legal documents on this subject at the African level. This does not mean that there is no African digital law. On the contrary, digital legal rules in Africa exist but do not keep pace with current technological developments.

The article also indicates that there is no need for the rules of digital law in the field of artificial intelligence to be collected in one law, but rather their spread to other branches of law reflects the multidisciplinary dimension of the ramifications of artificial intelligence imposed by practical practice. Finally, countries must work to enact explicit legislation on making the use of artificial intelligence more ethical, and they must work together within the framework of international cooperation to make such legislation consistent and consistent.

Acknowledgements

The authors are thankful to the Governance and Policy Design Research Lab (GPDRL) and to Prince Sultan University for providing APC for this publication.

References

- Albakjaji, M., & Almarzouqi, R. (2024). The Dilemma of the Copyrights of Artificial Intelligence: The Case of Saudi Arabia Regulations. *International Journal of Sociotechnology and Knowledge Development (IJSKD)*, 16(1), 1-15.
- Alsamara, T., & Ghazi, F. (2024). The impact of the legal framework of electronic payment on the digital economy. *Journal of Infrastructure, Policy and Development*, 8(7), 5936.
- Asongu, S. A., Singh, P., & Le Roux, S. (2018). Fighting software piracy: some global conditional policy instruments. *Journal of Business Ethics*, 152, 175-189.
- Baik, J. S. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics*, 52.
- Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. *Computer Science & IT Research Journal*, 5(3), 528-543.
- Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. *Computer Science & IT Research Journal*, 5(3), 528-543.
- Bakhramova, M. (2024). Harmonization of the Legal Framework for Online Arbitration. *International Journal of Law and Policy*, 2(2).
- Buiten, M. C. (2024). Product liability for defective AI. *European Journal of Law and Economics*, 1-35.
- Calvi, A. (2024). Data Protection Impact Assessment under the EU General Data Protection Regulation: A Feminist Reflection. *Computer Law & Security Review*, 53, 105950.
- Carlson, C. R., & Terry, C. (2024). The Devil's in the Details: How Countries' Defamation Laws Can (and Can't) Combat Hate Speech. *Journalism Practice*, 18(2), 242-264.
- Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International & Comparative Law Quarterly*, 69(4), 819-844.
- Chung, C. Y. (2010). The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth. *Harv. JL & Tech.*, 24, 233.
- Cortiz, D., & Zubiaga, A. (2020). Ethical and technical challenges of AI in tackling hate speech. *The International Review of Information Ethics*, 29.
- Dhali, M., Hassan, S., Zulhuda, S., & Bt Ismail, S. F. (2022). Artificial intelligence in health care: data protection concerns in Malaysia. *International Data Privacy Law*, 12(2), 143-161.
- Directive, C. (1985). Council 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. *Official Journal L*, 210(07/08), 0029-0033.
- Durneva, P. N., Perepadya, O. A., Stankevich, G. V., Pogodina, I. V., & Mayboroda, E. T. (2021). Civil law aspects of the phenomenon of artificial intelligence. *Advances in Research on Russian Business and Management*, 2021, 391-399.
- Elkadi, M. A. A. (2021). Implications of Artificial Intelligence Content Moderation on Free Speech: Regulating Automated Content Moderation Under International Human Rights Law Through A Comparative Lens (Doctoral dissertation, Department of Legal Studies, Central European University).
- Farouk, G., & Alsamara, T. (2023). Legal view on blockchain technologies in healthcare: A European states case study. *International Journal of Sociotechnology and Knowledge Development (IJSKD)*, 15(1), 1-13.
- Gaffar, H., & Albarashdi, S. (2024). Copyright Protection for AI-Generated Works: Exploring Originality and Ownership in a Digital Landscape. *Asian Journal of International Law*, 1-24.
- Goldman, L. (2012). Interpreting the Computer Fraud and Abuse Act. *Pitt. J. Tech. L. & Pol'y*, 13, 1.
- Harding, E. L., Vanto, J. J., Clark, R., Hannah Ji, L., & Ainsworth, S. C. (2019). Understanding the scope and impact of the california consumer privacy act of 2018. *Journal of Data Protection & Privacy*, 2(3), 234-253.
- Harrison, A. (2022). Where Next for the Right to Delete: Stepping Out of the Shadow of the Right to be Forgotten. *Fed. Comm. LJ*, 75, 319.
- Hassan, S., Dhali, M., Zaman, F., & Tanveer, M. (2021). Big data and predictive analytics in healthcare in Bangladesh: regulatory challenges. *Heliyon*, 7(6).
- Janow, M. E., & Mavroidis, P. C. (2019). Digital trade, e-commerce, the WTO and regional frameworks. *World Trade Review*, 18(S1), S1-S7.
- Joyce, A., & Javidroozi, V. (2024). Smart city development: Data sharing vs. data protection legislations. *Cities*, 148, 104859.
- Koen Jr, C. M., & Im, J. H. (1997). Software piracy and its legal implications. *Information & management*, 31(5), 265-272.
- Lee, S. H. (2024). Comments on the Amendments to the French Civil Code on Liability for Objects. *Law Journal*, 84, 239-270.
- Lepoutre, M., Vilar-Lluch, S., Borg, E., & Hansen, N. (2024). What is hate speech? The case for a corpus approach. *Criminal Law and Philosophy*, 18(2), 397-430.
- Lunney Jr, G. S. (2001). The death of copyright: Digital technology, private copying, and the digital millennium copyright act. *Virginia Law Review*, 813-920.
- Margono, S. (2024). Development Intellectual Property (Ip) Dispute Resolution In Digital Industries For Ip Attorneys As Legal Profession. *Journal of Namibian Studies: History Politics Culture*, 41, 31-62.
- Meltzer, J. P. (2019). Governing digital trade. *World Trade Review*, 18(S1), S23-S48.
- Naik, N., Hameed, B. M., Shetty, D. K., Swain, D., Shah, M., Paul, R., ... & Somani, B. K. (2022). Legal and ethical consideration in artificial intelligence in healthcare: who takes responsibility?. *Frontiers in surgery*, 9, 266.

- Navas, S. (2020). Producer liability for AI-based technologies in the European Union. *International Law Research*, 9(1), 77-84.
- Novruzova, O. B., Pronina, Y. O., Shergunova, E. A., & Gorevoy, E. D. (2020). The contract of power supply during the era of the digital law: civil bases. In *Scientific and Technical Revolution: Yesterday, Today and Tomorrow* (pp. 553-560). Springer International Publishing.
- Pardau, S. L. (2018). The california consumer privacy act: Towards a european-style privacy regime in the united states. *J. Tech. L. & Pol'y*, 23, 68.
- Rahman, F., & Pandey, P. (2020). Online Software Piracy and Its Related Laws. Available at SSRN 3648512.
- Regulation (EU) 2016/679 of the European parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), published on : <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>
- Ruddin, I., & SGN, S. Z. (2024). Evolution of Cybercrime Law in Legal Development in the Digital World. *Jurnal Multidisiplin Madani*, 4(1), 168-173.
- Sarabdeen, J., & Mohamed Ishak, M. M. (2024). A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR). *International Journal of Law and Management*.
- Schneeberger, D., Stöger, K., & Holzinger, A. (2020, August). The European legal framework for medical AI. In *International Cross-Domain Conference for Machine Learning and Knowledge Extraction* (pp. 209-226). Cham: Springer International Publishing.
- Schow, E. (2023). Updating the Berne Convention for the Internet Age: Un-Blurring the Line Between United States and Foreign Copyrighted Works. *Brigham Young University Journal of Public Law*, 37(2), 385-413.
- Schrock, A. R. (2019). What is civic tech? Defining a practice of technical pluralism. In *The right to the smart city* (pp. 125-133). Emerald Publishing Limited.
- Simmons, R. (2016). The failure of the Computer Fraud and Abuse Act: Time to take an administrative approach to regulating computer crime. *Geo. Wash. L. Rev.*, 84, 1703.
- Smirnova, Y., & Travieso-Morales, V. (2024). Understanding challenges of GDPR implementation in business enterprises: a systematic literature review. *International Journal of Law and Management*.
- Solum, L. B. (2020). Legal personhood for artificial intelligences. In *Machine ethics and robot ethics* (pp. 415-471). Routledge.
- Straub Jr, D. W., & Collins, R. W. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *Mis Quarterly*, 143-156.
- Sung, H. C. (2020). Can online courts promote access to justice? A case study of the internet courts in China. *Computer Law & Security Review*, 39, 105461.
- Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review*, 35(4).
- Vargas, E. T., & Torres, E. (2024). Legal Challenges of Digital Copyright Laws in the Circulation of Digital Content. *Law and Economy*, 3(1), 1-10.
- Widła, B. (2024). No More Convergence? Copyright Protection of Application Programming Interfaces in the USA and the EU. Copyright Protection of Application Programming Interfaces in the USA and the EU (June 15, 2023). Péter Mezei-Hannibal Travis-Anett Pogácsás: Harmonizing Intellectual Property Law for a Trans-Atlantic Knowledge Economy, Brill.
- Wuyts, D. (2014). The product liability directive—more than two decades of defective products in Europe. *Journal of European Tort Law*, 5(1), 1-34.