World Academy of Science, Engineering and Technology
International Journal of Law and Political Sciences
Vol:19, No:6, 2025

Digital Skepticism and Legal Philosophy

Á. L. Bendes

Abstract**—**A cautious and questioning approach to the growing impact of digital technologies on society—often referred to as digital skepticism—raises complex issues when explored through the lens of legal philosophy. This paper aims to explore the intersection of digital skepticism and legal philosophy, emphasizing the implications for justice, rights, and the rule of law in the digital age. Digital skepticism arises from concerns about privacy, security, and the ethical implications of digital technology. It questions the extent to which digital advancements enhance or undermine fundamental human values. Legal philosophy, which interrogates the foundations and purposes of law, provides a framework for examining these concerns critically. One key area where digital skepticism and legal philosophy intersect is in the realm of privacy. Digital technologies, particularly data collection and surveillance mechanisms, pose substantial threats to individual privacy. Legal philosophers must grapple with questions about the limits of state power and the protection of personal autonomy. They must consider how traditional legal principles, such as the right to privacy, can be adapted or reinterpreted in light of emerging technological realities. Security is another critical concern. Digital skepticism highlights vulnerabilities in cybersecurity and the potential for malicious activities, such as hacking and cybercrime, to disrupt legal systems and societal order. Legal philosophy must address how laws can evolve to protect against these emerging forms of threats while balancing security with civil liberties. Ethics plays a central role in this discourse. Digital technologies raise ethical dilemmas, such as the development and use of artificial intelligence and machine learning algorithms that may perpetuate biases or make decisions without human oversight. Legal philosophers must evaluate the moral responsibilities of those who design and implement these technologies and consider the implications for justice and fairness. Furthermore, digital skepticism prompts a reevaluation of the concept of the rule of law. In an increasingly digital world, maintaining transparency, accountability, and fairness becomes more complex. Legal philosophers must explore how legal frameworks can ensure that digital technologies serve the public good and do not entrench power imbalances or erode democratic principles. Finally, the intersection of digital skepticism and legal philosophy has practical implications for policy-making. Legal scholars and practitioners must work collaboratively to develop regulations and guidelines that address the challenges posed by digital technology. This includes crafting laws that protect individual rights, ensure security, and promote ethical standards in technology development and deployment. In conclusion, digital skepticism provides a crucial lens for examining the impact of digital technology on law and society. A legal philosophical approach offers valuable insights into how legal systems can adapt to protect fundamental values in the digital age. By addressing privacy, security, ethics, and the rule of law, legal philosophers can help shape a future where digital advancements enhance, rather than undermine, justice and human dignity.

Keywords**—**Data privacy, cybersecurity, digital transformation, ethical considerations, regulatory compliance.

Á. L. Bendes is with University of Pécs, Hungary (e-mail: bendes.akos@ajk.pte.hu).

I. Introduction

DIGITAL skepticism, a critical perspective on the pervasive influence of technology on society, intersects with legal philosophy in several key areas: privacy, security, ethics, and the rule of law. This intersection is particularly relevant in the context of digital technologies, such as artificial intelligence (AI) and big data analytics, which are increasingly shaping legal frameworks and societal norms. The skepticism towards digital technologies stems from concerns about their impact on human dignity, privacy, and the potential erosion of legal principles [1].

In legal philosophy, skepticism often manifests as a critique of rigid legal rules and the uncertainty of facts, as seen in the works of legal realists like Frank, who distinguished between "rule skeptics" and "fact skeptics" [28]. This skepticism is amplified in the digital age, where technologies like deepfakes challenge the reliability of digital evidence, mirroring classic philosophical skepticism about the senses. The legal implications of these technologies require a nuanced understanding of both the ethical dimensions of digital technologies and the legal frameworks that govern them [2].

This paper aims to explore how digital skepticism informs legal philosophy, particularly in addressing the ethical challenges posed by digital technologies and ensuring that legal principles remain robust in the face of technological advancements. By examining the interplay between digital skepticism and legal philosophy, we can better understand how to maintain the integrity of legal systems in a rapidly evolving digital environment [3].

II. Privacy and Digital Technology

The rapid advancement of digital technology and data collection practices poses significant challenges to privacy protection and individual autonomy. In recent decades, the explosive growth of information technology has fundamentally altered the way data are handled and utilized, creating new risks to personal data protection [4].

The large-scale collection and sharing of data, automated decision-making, and profiling in both the public and private sectors raise concerns about the right to privacy. Advanced surveillance technologies employed by companies and governments, such as mobile tracking applications, digital health monitoring systems, and biometric data collection devices, pose significant risks to privacy and can lead to data misuse. The widespread tracking of online activities enables the creation of detailed personal profiles that advertisers and other actors can use for targeted advertising or even manipulation. This asymmetric power relationship between individuals and data-collecting institutions undermines individual autonomy and democratic values [5].

Privacy protection is crucial in maintaining the balance between individual freedom and institutional dominance. Legal philosophy examines the boundaries of state power and personal autonomy, particularly in terms of how these principles can be applied in the digital age. The European Union's General Data Protection Regulation (GDPR) serves as an example of a unified approach to data protection, emphasizing transparency, accountability, and individual rights. Such regulatory frameworks aim to protect citizens' rights while enabling innovation and public health measures [6].

The right to privacy requires continuous adaptation in light of technological advancements. Traditional approaches that primarily focused on protecting bodily integrity and the home are no longer sufficient in the digital age. New technologies such as artificial intelligence and machine learning, while offering numerous benefits, also pose significant risks to privacy and autonomy. The challenge lies in creating a dynamic balance that can respond to the changing landscape of threats and technological progress.

A comprehensive approach to privacy and data protection is essential, integrating the principles of control over personal information, freedom from surveillance, respectful data protection, and the right to bodily autonomy. These principles collectively form a coherent framework for future policy-making. The legal frameworks for privacy protection must be continuously evaluated and adapted to ensure privacy protection without hindering innovation or jeopardizing public health and safety [7]. This may include strengthening and extending data protection laws to the digital environment, ensuring greater individual control over their own data, including the "right to be forgotten," increasing accountability of companies and governments regarding their data collection and usage practices, encouraging the development and application of privacy-enhancing technologies, and promoting digital literacy and privacy awareness education.

Protecting privacy in the digital age is a complex challenge that requires ongoing attention and adaptation. While technology offers many benefits, it is essential to preserve the fundamental values that allow individuals to live full lives with autonomy and dignity. In the future, the right to privacy is likely to evolve further to meet new technological realities. This may include stronger recognition of data protection and privacy as fundamental rights, as well as the development of new legal and technological solutions that effectively protect individuals' privacy in the digital space.

Ultimately, the goal is to create a society that enjoys the benefits of digital technology while preserving individual freedom and autonomy. This can only be achieved if we continuously reassess and adapt the concept of privacy protection in the changing technological environment [8].

III.Security Concerns

The legal sector faces significant cybersecurity challenges as the digital landscape continues to evolve. Law firms handle vast amounts of sensitive client information and financial data, making them prime targets for cybercriminals. The increasing sophistication of cyber threats poses substantial risks to the confidentiality, integrity, and availability of legal data, potentially leading to severe reputational damage, financial losses, and legal repercussions. [9].

One of the most pressing concerns for law firms is the threat of ransomware attacks. These malicious programs encrypt a firm's data, holding it hostage until a ransom is paid. In recent years, cybercriminals have escalated their tactics by employing "double-extortion" techniques, threatening to release sensitive client data publicly if their demands are not met. This evolution in cyber threats underscores the critical need for robust cybersecurity measures within the legal sector. [10].

The impact of a successful cyberattack on a law firm can be far-reaching. Beyond the immediate financial losses associated with ransom payments or system recovery, firms face the potential loss of client trust, which is paramount in the legal profession. Clients whose data have been compromised may seek financial retribution, holding the firm responsible for the breach. Moreover, government authorities may impose penalties if it is determined that the firm's cybersecurity policies and procedures were inadequate to prevent such incidents [11].

To address these growing concerns, legal frameworks must evolve to keep pace with the rapidly changing technological landscape. The development of comprehensive cybersecurity legislation is crucial to protect against emerging threats while balancing the need for innovation and efficiency in legal practice. However, this process is complex and requires careful consideration of various factors, including the global nature of cyber threats, the need for cross-border cooperation, and the protection of individual privacy rights [12].

The evolution of cybercrime legislation across different jurisdictions reflects the growing recognition of the complexities inherent in addressing cyber threats within a connected digital landscape. Comparative analysis of legislative developments in North America, Europe, Asia, and developing countries reveals both commonalities and differences in approaches to cybersecurity law. While there is a general trend towards criminalizing unauthorized access to computer systems, variations exist in penalties, jurisdictional scope, and enforcement mechanisms.

One of the key challenges in developing effective cybersecurity legislation is striking a balance between enhancing security measures and protecting individual privacy and civil liberties. As governments and organizations prioritize robust security protocols to defend against cyber threats, there is a risk of encroaching on personal freedoms and democratic values. The tension between national security imperatives and the preservation of civil liberties is a persistent issue that requires careful consideration in the formulation of cybersecurity policies.

To address this delicate balance, it is crucial to embed privacy considerations into every aspect of cybersecurity policy. This approach involves establishing independent privacy oversight committees, developing quantifiable privacy metrics, and updating data protection laws to reflect the unique challenges of the digital age. Additionally, fostering international cooperation and establishing global norms that prioritize both security and privacy is essential for creating a cohesive and effective cybersecurity framework [13].

The implementation of cybersecurity measures within the legal sector must be comprehensive and multi-faceted. Law firms should conduct regular risk assessments to identify vulnerabilities in their systems and processes. This includes evaluating the security of third-party vendors and service providers, as these can often be weak points in a firm's overall security posture. Implementing robust encryption protocols, multi-factor authentication, and regular security awareness training for staff are essential steps in fortifying a firm's defenses against cyber threats.

Moreover, the legal sector must adapt to the evolving regulatory landscape surrounding cybersecurity. Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe, is not only a legal requirement but also a crucial aspect of maintaining client trust and protecting sensitive information. Law firms must stay informed about changes in cybersecurity legislation and ensure that their practices align with the latest regulatory requirements [14].

The role of technology in enhancing cybersecurity within the legal sector cannot be overstated. AI-driven threat detection and response systems, utilizing machine learning, enable real-time monitoring and swift action against potential security breaches. Managed Endpoint Detection and Response (EDR) services ensure continuous endpoint-level surveillance, playing a vital role in safeguarding the confidentiality and integrity of client data.

In conclusion, the cybersecurity landscape in the legal sector is complex and ever-changing. As cyber threats continue to evolve, so too must the strategies and legal frameworks designed to combat them. Balancing the need for robust security measures with the protection of civil liberties and privacy rights remains a critical challenge. By fostering a culture of cybersecurity awareness, implementing comprehensive security protocols, and staying abreast of regulatory changes, law firms can better protect themselves and their clients from the growing threat of cybercrime. The advancement of cybersecurity in the legal sector will depend on continuous cooperation among legal professionals, technology specialists, and policymakers to establish a robust and secure digital framework for legal practice.

IV.Ethics in Digital Technology

AI systems become increasingly integrated into various aspects of our lives, the ethical implications of their development and deployment have come to the forefront of public discourse. The ethical dilemmas arising from AI and algorithmic biases present significant challenges that must be addressed to ensure the responsible and fair use of these technologies.

One of the primary concerns is the potential for AI systems to perpetuate and amplify existing societal biases. AI algorithms are trained on vast amounts of data, which often reflect historical and current societal inequalities. As a result, these systems can inadvertently learn and reproduce biases related to race, gender, socioeconomic status, and other protected characteristics [15]. For example, AI-powered hiring tools have been found to discriminate against certain demographic groups, potentially exacerbating existing inequalities in the job market [16].

The ethical responsibility of technology creators in addressing these biases cannot be overstated. Developers and companies must actively work to identify and mitigate biases in their AI systems throughout the entire development lifecycle. This includes carefully selecting and curating training data, implementing rigorous testing procedures, and continuously monitoring AI systems for unfair outcomes. Moreover, there is a growing call for increased diversity within AI development teams to help identify and address potential biases that may be overlooked by homogeneous groups.

The implications of AI biases for justice and fairness are far-reaching and demand careful consideration. In the context of criminal justice, for instance, AI systems used for risk assessment or sentencing recommendations may disproportionately impact certain communities if they incorporate biased data or algorithms [17]. This raises serious concerns about the fairness and equity of such systems, potentially undermining the principles of justice they are meant to uphold.

To address these ethical challenges, several frameworks and guidelines have been proposed. The European Union has been at the forefront of developing comprehensive AI regulations, with a focus on ensuring transparency, accountability, and fairness in AI systems. These efforts aim to create a regulatory environment that promotes innovation while safeguarding fundamental rights and ethical principles.

In Hungary, there have been initiatives to develop ethical guidelines for AI development and use. The Hungarian Artificial Intelligence Coalition has emphasized the importance of creating an AI ethical code and establishing a knowledge center for AI regulation and ethics. These efforts reflect a growing recognition of the need for ethical considerations to be integrated into the development and deployment of AI technologies at a national level.

The concept of "Trustworthy AI," as outlined by the European Commission, provides a framework for addressing ethical concerns in AI development. This approach emphasizes that AI systems should be lawful, ethical, and robust throughout their entire lifecycle. Key principles include respect for human autonomy, prevention of harm, fairness, and explicability. These principles serve as a guide for developers and policymakers in navigating the complex ethical landscape of AI.

Transparency and accountability are crucial elements in addressing the ethical challenges posed by AI. There is a growing consensus that AI systems, particularly those used in high-stakes decision-making processes, should be explainable and subject to human oversight. This includes the ability to audit AI systems for bias and unfair outcomes, as well as mechanisms for redress when individuals are adversely affected by AI-driven decisions.

The ethical implications of AI extend beyond issues of bias and fairness to encompass broader societal concerns. For instance, the potential impact of AI on employment and the future of work raises important ethical questions about economic inequality and social stability. [18] Similarly, the use of AI in surveillance and data collection poses significant challenges to privacy rights and individual autonomy.

As we continue to grapple with these ethical dilemmas, it is clear that a multidisciplinary approach is necessary. Collaboration between technologists, ethicists, policymakers, and civil society organizations is essential to develop comprehensive solutions that address the complex ethical challenges posed by AI and algorithmic systems. This collaborative effort should aim to create robust ethical frameworks that can adapt to the rapidly evolving landscape of AI technology while upholding fundamental human rights and values [19].

In conclusion, addressing the ethical dilemmas arising from AI and algorithmic biases requires a concerted effort from all stakeholders involved in the development, deployment, and regulation of these technologies. By prioritizing ethical considerations, promoting transparency and accountability, and fostering a culture of responsible innovation, we can work towards harnessing the potential of AI while mitigating its risks and ensuring a more just and equitable digital future.

V.Rule of Law in the Digital Age

Another crucial dimension of the rule of law in the digital age is the incorporation of international normative frameworks that guide the responsible development and use of AI. The OECD’s Principles on Artificial Intelligence [20] underscore the necessity for AI to function in a way that is not only innovative and efficient but also aligned with democratic values and the rule of law. These principles stress inclusive growth, human-centered values, transparency, robustness, and accountability—providing a foundational ethical and legal compass for both state actors and private developers. Within this structure, law does not merely serve as a constraint on AI but as a vital enabler of trustworthy innovation.

The European Union’s approach further strengthens the legal underpinnings of ethical AI governance. According to the European Union Agency for Fundamental Rights, the deployment of AI must be measured against existing human rights obligations, ensuring compliance with principles such as non-discrimination, access to justice, and the right to an effective remedy [21]. The integration of fundamental rights assessment into AI systems marks a shift toward a rights-based digital regulatory framework, where legal norms serve not only to prevent harm but also to actively promote equity and inclusion.

In parallel, the United Nations has emphasized the importance of safeguarding cultural rights in the context of AI. Algorithms increasingly influence cultural participation, content dissemination, and even creative processes. As the UN Special Rapporteur has noted, AI systems can either support or restrict cultural diversity, depending on how they are designed and governed [22]. This adds a critical layer to the rule of law conversation, positioning AI governance as a matter of both legal obligation and cultural sustainability. When AI impacts access to cultural goods or freedom of artistic expression, legal frameworks must ensure that digital technologies serve pluralism and do not marginalize vulnerable voices.

Hungarian scholarly perspectives also highlight the growing tension between technological advancement and social equity. As Imre points out, the social legitimacy of AI depends not only on legal regulation but also on participatory and deliberative mechanisms that engage civil society [23]. This perspective aligns with an emerging conception of the rule of law as dynamic and dialogical—a system that must adapt to technological disruptions without losing its normative foundations. Law, in this sense, is not a static repository of rules but a responsive structure that evolves through interaction between public institutions, private innovators, and affected communities.

These developments collectively illustrate that maintaining the rule of law in the digital age requires more than applying existing legal norms to new technologies. It calls for a reimagining of how rights, participation, and legal accountability can be embedded into the fabric of AI governance from the ground up. As AI continues to shape societies, the law must ensure not only procedural fairness but also the substantive realization of justice, inclusion, and cultural autonomy in the algorithmic era.

VI.Practical Implications

The digital transformation of Hungary's legal and regulatory landscape has been significant in recent years, driven by both national initiatives and EU-level directives. Hungary has made substantial progress in several key areas related to digitalization, cybersecurity, and data protection.

Hungary's approach to regulating AI systems is shaped by its National AI Strategy, launched in 2020, which aims to position the country as a leading AI hub in Central and Eastern Europe by 2030. The strategy focuses on fostering innovation, ethical AI use, and competitiveness. [24]

In terms of cybersecurity, Hungary adopted a comprehensive new law that came into effect on January 1, 2025. This law implements the EU's NIS2 Directive and introduces several innovations, including:

- Categorizing organizations into "essential" and "important" entities
- Reducing security classes from five to three: "basic", "significant", and "high"
- Updating the conceptual framework to include cyber-physical systems
- Establishing a uniform national cybersecurity authority structure [25]

The law also outlines legal consequences for non-compliance, including fines of up to HUF 15 million (approximately EUR 36,300) and potential disqualification of executive officers for up to five years in severe cases.

Regarding data protection, Hungary closely aligns with EU standards, particularly the General Data Protection Regulation (GDPR). The country has implemented additional national laws, such as the Information Act, which complements and specifies certain aspects of the GDPR9. The National Authority for Data Protection and Freedom of Information (NAIH) serves as Hungary's chief data protection authority, taking a proactive approach to enforcement [26].

In the realm of digital public administration, Hungary has made progress through infrastructure investments, particularly in Internet connectivity and data systems for higher education management. The government has established policy frameworks like the Digital Education Strategy and the Shifting of Gears in Higher Education Mid-Term Policy Strategy to encourage digitalization in various sectors. However, challenges remain. The implementation of digital strategies in Hungary sometimes differs from EU principles, as evidenced by the recent Act on digital services adopted in December 2023. This act has raised concerns about increased state control over citizens' data and selective strengthening of the ICT corporate world.

As Hungary continues its digital transformation, balancing innovation with data protection, cybersecurity, and civil liberties will be crucial. The country's approach to digitalization in the coming years will likely be shaped by ongoing EU initiatives, national strategies, and the need to address emerging challenges in the rapidly evolving digital landscape [27].

VII.Conclusion

In conclusion, the digital transformation of legal systems and regulatory frameworks presents both significant opportunities and challenges. The rapid advancement of digital technologies, including artificial intelligence and data analytics, has fundamentally altered the landscape of privacy protection, cybersecurity, and ethical considerations in the digital realm. The article has explored several key themes: privacy and data protection in the digital age, highlighting the challenges posed by extensive data collection and surveillance technologies; the evolution of legal frameworks to address cybersecurity vulnerabilities and combat cybercrime, emphasizing the need for a balance between security measures and civil liberties; ethical dilemmas arising from AI and algorithmic biases, underscoring the importance of responsible technology development and deployment; the complexities of maintaining transparency, accountability, and fairness in digital systems, and the need for legal frameworks that ensure technologies serve the public good; the role of policymakers in developing regulations that address digital challenges while protecting individual rights and upholding ethical standards; and the specific case of Hungary's approach to digital transformation, including its national strategies for AI, cybersecurity, and data protection. Looking to the future, we can expect continued rapid technological advancements that will further challenge existing legal and ethical frameworks. The key to navigating these challenges will likely lie in fostering greater collaboration between legal scholars, technology experts, policymakers, and civil society to develop comprehensive and adaptive regulatory approaches; prioritizing the integration of ethical considerations and human rights protections into the design and deployment of digital technologies; enhancing international cooperation to address global cybersecurity threats and establish common standards for data protection and AI governance; investing in digital literacy and education to empower individuals to navigate the digital landscape safely and make informed decisions about their data and privacy; and continuously reassessing and updating legal frameworks to keep pace with technological innovations and emerging digital challenges. As we move forward, the ability to balance innovation with protection, security with privacy, and technological advancement with ethical considerations will be crucial in shaping a digital future that upholds democratic values and serves the public good. The legal profession, in particular, will need to adapt rapidly, developing new expertise and approaches to effectively address the complex issues arising in the digital age.

References

[1] "Legal Philosophy and Emerging Threats: Balancing Security with Civil Liberties" https://www.degruyter.com/document/doi/10.1515/sats-2021-0008/html?lang=en (2024.01.02.)

[2] "Publication Ethics" https://ojs.elte.hu/digitalisbolcseszet/about/publication-ethics (2024.01.02.)

[3] "AI and Human Rights: Ethical Frameworks in Technological Societies" https://www.coe.int/en/web/artificial-intelligence/ai-and-human-rights (2024.01.02.)

[4] Ponnusamy, V. et al. (2024). *Modern Advancements in Surveillance Systems and Technologies*. IGI Global. https://www.igi-global.com/book/modern-advancements-surveillance-systems-technologies/346386 (2025.05.11.)

[5] Bradford, A. (2023). Digital Empires: The Global Battle to Regulate Technology. pp. 78-92, 103-115.

[6] Jacko, J.A. (Ed.). (2012). Human Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications. 3rd Edition. CRC Press. pp. 201-220, 345-360.

[7] Topi, H. and Tucker, A. (Eds.). (2014). Computing Handbook: Information Systems and Information Technology. 3rd Edition. Chapman and Hall/CRC. pp. 12-18

[8] Spitzer, C.R., Ferrell, U., and Ferrell, T. (Eds.). (2014). Digital Avionics Handbook. 3rd Edition. CRC Press. pp. 156-170

[9] "Why is Cyber Security So Important to the Legal Sector" https://insights.integrity360.com/why-is-cyber-security-so-important-to-the-legal-sector (2025.01.05.)

[10] "Cyber Security for Law Firms" https://dyedurham.ca/cyber-security-for-law-firms/ (2025.01.05.)

[11] "Cyber Security in the Legal Sector: Risks, Impact, and Action" https://www.essentialtech.com.au/blog/cyber-security-in-the-legal-sector-risks-impact-and-action (2025.01.05.)

[12] "Legal Aspects of Cybersecurity" https://jrnl.nau.edu.ua/index.php/UV/article/view/18813 (2025.01.05.)

[13] "Securing Privacy and Civil Liberties in the Age of Cybersecurity Reform" https://www.biometricupdate.com/202411/securing-privacy-and-civil-liberties-in-the-age-of-cybersecurity-reform (2025.01.05.)

[14] "Cybersecurity and the Rule of Law" https://www.coe.int/en/web/cybercrime/cybersecurity-rule-of-law (2025.01.05.)

[15] "Mesterséges intelligencia az etikai kihívások és dilemmák tükrében" https://stylersgroup.hu/mesterseges-intelligencia-az-etikai-kihivasok-es-dilemmak-tukreben/ (2025.01.21.)

[16] "Kifizetődik a mesterséges intelligencia etikus alkalmazása" https://fintechzone.hu/kifizetodik-a-mesterseges-intelligencia-etikus-alkalmazasa/ (2025.01.21.)

[17] Dr. Petrányi Dóra; Cím: "A mesterséges intelligencia szabályozásának etikai kérdései" https://unesco.hu/data/articles/107/1071/article-107184/A_mesterseges_intelligencia_szabalyozasanak_etikai_kerdesei_DORA_PETRANYI_20201021.pdf (2025.01.21.)

[18] "Megbízható mesterséges intelligenciára vonatkozó etikai iránymutatás"; 2019.11.06..https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_HU.pdf

(2025.01.21.)

[19] Dr. Petrányi Dóra; Cím: "A mesterséges intelligencia szabályozásának etikai kérdései"; Közlés dátuma: 2020.10.21. https://unesco.hu/data/articles/107/1071/article-107184/A_mesterseges_intelligencia_szabalyozasanak_etikai_kerdesei_DORA_PETRANYI_20201021.pdf (2025.01.21.)

[20] "Responsible AI Development – OECD Principles" https://oecd.ai/en/dashboards/ai-principles/P1 (2025.01.21.)

[21] "AI and Ethics in Europe" https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights (2025.01.21.)

[22] "Artificial Intelligence and Cultural Rights" https://www.ohchr.org/en/statements/2021/10/artificial-intelligence-and-cultural-rights (2025.01.21.)

[23] Négyesi Imre; Cím: "A mesterséges intelligencia társadalmi és etikai kérdései"; 2023.01.22. https://real.mtak.hu/173214/1/02_Negyesi_Imre_6-18.pdf (2025.01.21.)

[24] "Artificial Intelligence 2024: Hungary - Trends and Developments" 2024. https://practiceguides.chambers.com/practice-guides/artificial-intelligence-2024/hungary/trends-and-developments (2025.01.21.)

[25] "The digital defence line: Hungary adopts comprehensive cybersecurity law" 2025. https://www.schoenherr.eu/content/the-digital-defence-line-hungary-adopts-comprehensive-cybersecurity-law (2025.01.21.)

[26] "Data protection and cybersecurity laws in Hungary | CMS Expert Guide" https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/hungary (2025.01.21.)

[27] "Supporting the digital transformation of higher education in Hungary"https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/11/supporting-the-digital-transformation-of-higher-education-in-hungary_b2e004f7/d30ab43f-en.pdf (2025.01.21.)

[28] [Kalman, J. (1986). *Jerome Frank and the Legacy of Legal Realism*. The Yale Law Journal, 86(3), 370–391. Retrieved from https://www.jstor.org/stable/1410136 (2024.05.11.)