



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS
TÉZISFÜZETE

DR. ANTAL TÍMEA

A compliance és a mesterséges intelligencia kölcsonhatásai

Témavezető: Dr. Számadó Róza Zsuzsánna

BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA

Budapest, 2026. április 20.

Tartalomjegyzék

1	Summary	3
2	A kutatás előzményei	4
3	Célkitűzések	5
4	Vizsgálati módszerek	6
5	Új tudományos eredmények.....	7
6	Az eredmények hasznosítási lehetősége	8
7	Irodalmi hivatkozások listája/ Irodalomjegyzék	9
8	A tézispontokhoz kapcsolódó tudományos közlemények	18

1 Summary

This doctoral dissertation aims to examine the interactions between compliance and artificial intelligence. The topic is highly relevant due to the rapid advancement of digital transformation and artificial intelligence, which, in addition to transforming organizational operations, is generating new types of security and regulatory challenges. In this environment, compliance is a key tool for risk management and operational regulation; however, an integrated examination of these two areas is not yet consistent in the literature. The study is based on three main questions: the definability of the concept of compliance, the practical characteristics of artificial intelligence and compliance, and the methodological and organizational solutions supporting their application. The research employs a mixed-methods approach: secondary research is based on a review of the literature, while primary research examines domestic practices through a questionnaire survey and expert interviews. The empirical analysis uses statistical methods to uncover correlations.

The results contribute to the development of the field at the theoretical, empirical, and practical levels. At the theoretical level, it can be established that the concept of compliance is not uniform but rather a dynamically evolving, multidimensional phenomenon that, in the digital environment, can increasingly be interpreted as a risk-sensitive and security-oriented governance framework. The focus of the compliance function is shifting from a monitoring role toward a preventive and supportive one.

Empirical evidence shows that the use of artificial intelligence tools is significantly correlated with the presence of compliance systems: companies that use such technologies are more likely to have formalized compliance policies. The implementation of compliance also strengthens organizational security awareness, which is supported by the existence of policies, their review, and training. The study identifies three key risk areas in the application of artificial intelligence: data reliability, decision quality, and the lack of necessary competencies. From a practical perspective, the research results in a set of recommendations and a framework that supports the safe and regulated use of artificial intelligence. The findings highlight that compliance works effectively when it is embedded in the organizational culture and enforced at all levels of operations. The dissertation contributes to a reinterpretation of the concept of compliance and a deeper understanding of the relationship between artificial intelligence and compliance, and provides practical guidance for organizations on establishing safe, risk-sensitive operations.

2 A kutatás előzményei

A XXI. századi vállalati működés egyik meghatározó jellemzője a gyorsan változó technológiai és gazdasági környezet, amely fokozott alkalmazkodóképességet és rugalmas működést követel meg a szervezetektől. Az információs és kommunikációs technológiák fejlődése, valamint a mesterséges intelligencia térnyerése alapvetően alakítja át a szervezeti működést, a döntéshozatali folyamatokat és a kockázati struktúrákat.

A kutatás központjában a compliance és a mesterséges intelligencia kölcsönhatásainak vizsgálata áll. A compliance és a mesterséges intelligencia két új, a tudomány által egyre behatóbban vizsgált terület. Számos kutatás foglalkozik külön-külön ezekkel a témákkal, azonban kapcsolatuk vizsgálata jelenleg nem egységesen kidolgozott. Mind a két téma „hiper-interdiszciplináris” megközelítést igényel a kutatótól (közgazdaságtudomány–jogtudomány–informatika–szervezés–vezetéstudomány), hiszen piaci térnyerésük a mindennapi munkaköri gyakorlatban érhető tetten. Álláspontom szerint mind a compliance, mind a mesterséges intelligencia a tudomány és a gyakorlati alkalmazás számára egyaránt kulcsfontosságú. A megfelelés szükséges a mesterséges intelligencia alkalmazásához; a mesterséges intelligenciát lehet használni megfelelési feladatok ellátására is, tehát kétirányú kapcsolatot lehet meghatározni közöttük. A mesterséges intelligencia mint eszköz és mint kockázati tényező is szerepelhet egy magas színvonalú compliance rendszerben.

A fenti tényezők együttesen arra a tudományos problémára mutatnak rá, hogy a compliance és a mesterséges intelligencia kapcsolatának vizsgálata jelenleg széttagolt, és nem áll rendelkezésre olyan egységes elméleti és gyakorlati keret, amely képes kezelni a mesterséges intelligencia által generált kockázatokat.

Ez a kutatási kontextus indokolja a compliance fogalmának átfogóbb, többdimenziós vizsgálatát, a megfelelőség gyakorlati alkalmazásának, valamint a mesterséges intelligencián alapuló használatának elemzését a magyar vállalkozások esetében; valamint gyakorlati segédletek készítését.

3 Célkitűzések

A kutatás fő célja a megfelelőség és a mesterséges intelligencia kölcsönhatásait tudományos igényű elemzéssel vizsgálni. Ennek keretében cél egyrészt a compliance átfogó fogalommagyarázatát meghatározni szakirodalmi, elméleti kutatásra, funkciókra alapozva; másrészt kérdőíves módszerrel és interjú alkalmazásával elemezni a megfelelőség gyakorlati alkalmazását, valamint a mesterséges intelligencián alapuló használatának jellemzőit a magyar vállalkozások esetében; harmadrészt gyakorlati segédleteket készíteni ajánlások és compliance keretrendszer formájában annak érdekében, hogy a biztonsági szempontok előtérbe kerüljenek a mesterséges intelligencia alkalmazásából fakadó kockázatok kezelése során.

A téma jelentősége abban rejlik, hogy a XXI. században a vállalatok alkalmazkodóképessége és rugalmas működése alapvető feltétele a hosszú távú sikernek. A szervezetek működésük során folyamatosan szembesülnek a kihívások széles körével: az információs és kommunikációs technológiák (IKT) térnyerésétől kezdve, a felhalmozott és folyamatosan bővülő saját adatvagyon kezelésén, továbbá a munkaszervezési, és/vagy a humán erőforrás-képesség fejlesztésén át. A változó környezethez való alkalmazkodás során a kockázatok minimalizálását, a biztonság erősítését szolgálja a compliance (megfelelőség). A mesterséges intelligencia térnyerése új dimenziókat nyit a vállalati működésben: egyrészt jelentős hatékonyságnövelési lehetőségeket kínál, másrészt új versenyhelyzetet és egyben új típusú kockázatokat is teremt. A compliance hiánya biztonsági kockázat a vállalatra nézve a mesterséges intelligencia képességeivel szemben. A vállalkozásoknak nyitottnak kell lenni a modern kihívásokra, és lehetőleg a változások tudatos alakítóivá kell válniuk annak érdekében, hogy ne elszenvedői, hanem olyan befolyásolói legyenek a körülményeknek, amelyek előnyükre képesek fordítani a külső behatásokat.

A kutatás hozzájárul a compliance fogalmának újraértelmezéséhez, valamint a mesterséges intelligencia biztonságos és szabályozott alkalmazásának támogatásához.

4 Vizsgálati módszerek

Kutatómunkám során törekedtem az elméleti összefüggések és a gyakorlati eljárások komplex vizsgálatára, valamint kvantitatív és kvalitatív kutatási módszereket is alkalmaztam. A szakirodalom és a szabályozási kereteket bemutató dokumentumok elemzésének fő oka a kutatás megalapozása és az eredmények rendszerbe illesztése volt. A nemzetközi és a hazai stratégiai irányt tartalmazó dokumentumokat és tudományos cikkeket dolgoztam fel.

A compliance fogalmának elemzésekor egyrészt a használatban lévő angol nyelvű kifejezéseket vizsgáltam a biztonság fogalmával együtt, majd bibliometriai eszközök (Web of Science és a Magyar Tudományos Művek Tára nevű adatbázisok) alkalmazásával kísérletet tettem a compliance definiálására 2017-2024 időszakra, majd a 2025. évet is vizsgálva. Másrészt azt vizsgáltam az OpenAlex adatbázisban, hogy mely tudományterületek keretein belül született a legtöbb szakmai elemzés a compliance témájában 2017-2024 időszakban, majd a 2025. évben. A műhelyvitát követően a 2025. év elemzésbe történő bevonása indokoltá vált, figyelemmel arra, hogy a vizsgált terület dinamikus fejlődése és gyors változása befolyásolhatja a tézisek tartalmát.

Az elméleti és a szabályozási keretekre építve alkalmaztam a második kutatási módszert, vagyis a kérdőívezést. Adatfelvételt (MS Forms) végeztem online, önkitöltős módszerrel 2024. 11. 07. és 2024. 12. 16. között. A kérdőív 35 kérdést tartalmazott, melyek között szerepeltek nyitott és zárt kérdések egyaránt. A statisztikai elemzéseket az SPSS 30.0 (SPSS Inc., Chicago, Illions, USA) és MS Excel segítségével készítettem. A kérdőívet 139 fő töltötte ki, nem reprezentatív a kérdőív minta. A harmadik módszer 10 strukturált szakértői interjú készítése volt, 15 kérdés mentén, 60–80 perc közötti időtartamban. A kérdések sorrendje kötött volt, az interjúvázlatban lévő kérdések jelentős részére kötelezően választ vártam. Az interjúkat Microsoft Teams vagy telefonos hangrögzítés funkcióval rögzítettem, majd Microsoft Wordbe ültettem át a tartalmat.

A doktori értekezésben nem foglalkozom az adatvédelem témakörével, az Environmental (környezeti), Social (társadalmi) és Governance (irányítási) keretrendszerrel – ESG-vel, továbbá a digitális piacokról szóló jogszabállyal, a NIS2 uniós kiberbiztonsági irányelvvel és a hozzá kapcsolódó szabályozással sem. Ennek oka egyrészt az, hogy a fent említettek a kutatás célrendszerével csak közvetett kapcsolatban állnak, másrészt ezen adatok feldolgozása meghaladná az értekezés keretét.

5 Új tudományos eredmények

T1. Megállapítottam, hogy a compliance fogalma fejlődésen ment keresztül, tartalmában kiszélesedett, és új értelmezési keretben határozható meg. A compliance újraértelmezett fogalma: A compliance a szervezeti működés dinamikus, integratív és kockázátérzékeny irányítási rendszere, amely a normatív, szervezeti és technológiai dimenziók összehangolásán keresztül biztosítja a működés szabályozottságát és a kockázatok proaktív kezelését a digitális, adatvezérelt környezetben.

T2. Igazoltam, hogy a compliance funkciója a kontroll jellegű megközelítésről a szolgáltató és megelőző szerep irányába mozdult el.

T3. Empirikusan kimutattam, hogy a mesterséges intelligencia eszközhasználata és a compliance rendszerek jelenléte között szignifikáns kapcsolat áll fenn a hazai vállalkozások esetében.

T4. Bizonyítottam, hogy a compliance rendszerek alkalmazása növeli a szervezeti biztonságtudatot a mesterséges intelligencia használata során.

T5. Megállapítottam, hogy a munkavállalók biztonságtudata szervezeti szinten erősíthető a compliance szabályozás kialakításával és rendszeres felülvizsgálatával, valamint célzott, gyakorlatorientált képzések alkalmazásával

T6. Azonosítottam a mesterséges intelligencia alkalmazásához kapcsolódó főbb kockázattípusokat, és meghatároztam azok lehetséges compliance alapú kezelési módjait.

T7. Megállapítottam, hogy a compliance szervezeti kultúrába való beágyazódása alapvető feltétele a hatékony működésnek.

T8. Kidolgoztam egy közvetlenül alkalmazható compliance ajánlás rendszert.

T9. Kidolgoztam egy gyakorlati compliance keretrendszert, amely alkalmas a mesterséges intelligencia alkalmazásából fakadó kockázatok kezelésére.

6 Az eredmények hasznosítási lehetősége

A kutatás eredményei közvetlen gyakorlati hasznosíthatósággal bírnak, különösen a compliance rendszerek fejlesztése és a mesterséges intelligencia biztonságos szervezeti alkalmazása területén. A dolgozat egyik legfontosabb hozzájárulása, hogy a compliance és a mesterséges intelligencia összekapcsolását nemcsak elméleti, hanem operatív szinten is értelmezhetővé teszi.

A kutatás keretében kidolgozott ajánlások egyrészt meghatározzák a mesterséges intelligencia alkalmazása során vizsgálandó módszertani kérdéseket, másrészt konkrét iránymutatást adnak a compliance szempontú használatra, valamint bemutatják a mesterséges intelligencia alkalmazhatóságát a compliance feladatok támogatásában.

A dolgozat kiemelt gyakorlati eredménye egy strukturált compliance keretrendszer, amely hat kulcsfontosságú intézkedési területen – a szervezeti működéstől a kockázatmenedzsmenten és szabályozáson át a felelősségi rendszerig és képzésig – egységes logika mentén határozza meg a szükséges követelményeket. A keretrendszer újdonsága abban rejlik, hogy a hagyományosan nehezen alkalmazható szabályzati megközelítést rendszerszintű, folyamatorientált sablonokká alakítja át.

A sablonok pontosan definiálják a célkitűzéseket, szerepköröket, bemeneteket, folyamatlépéseket, kimeneteket, ellenőrzési pontokat és mérőszámokat, valamint beépítik a folyamatos fejlesztést biztosító PDCA logikát. Ezáltal a keretrendszer nemcsak szabályozási eszközként, hanem működési és irányítási támogatásként is alkalmazható.

A kidolgozott megközelítés hozzájárul a szervezeti biztonságtudat növeléséhez, támogatja a döntéshozókat a megfelelő szabályozási és működési megoldások kialakításában, valamint elősegíti a mesterséges intelligencia alkalmazásából fakadó kockázatok rendszerszintű kezelését. A keretrendszer adaptálható különböző szervezeti és ágazati környezetekben, ezáltal széles körben hasznosítható a gyakorlatban.

A kutatás továbbá alapot biztosít további tudományos vizsgálatok számára, különösen a mesterséges intelligencia és a compliance kapcsolatának nemzetközi és szektorspecifikus elemzése területén.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

- [1] Európai Bizottság: Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027 COM(2018) 434 final, 2018/0227(COD); <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN>
- [2] Európai Bizottság. (2025). *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future* (COM(2025) 290 final). Európai Bizottság.
- [3] European Union Agency for Cybersecurity. (2023). Cybersecurity threats fast forward 2030., https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030_1
- [4] Benedek P. (2012). Compliance Management – a New Response to Legal and Business Challenges. *Acta Polytechnica Hungarica*, 9(3), 135–148.
- [5] Huang, C., Zhang, Z., Mao, B. és Yao, X. (2023). An Overview of Artificial Intelligence Ethics. *IEEE Transactions on Artificial Intelligence*, 4(4), 799–819. <https://doi.org/10.1109/TAI.2022.3194503>
- [6] Gaudemet, A. (2020). What is Compliance? *RED*, 2020(1), 89–92. <https://doi.org/10.3917/red.001.0089>
- [7] Bygrave, L. A. (2022). Automating Compliance: Artificial Intelligence and the Future of Legal Oversight. *Computer Law & Security Review*, 47, Article 105701. <https://doi.org/10.1016/j.clsr.2022.105701>
- [8] Sloane, M., Moss, A. és Chowdhury, M. (2022). Participation is not a design fix for machine learning. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2), 1–20. <https://doi.org/10.1145/3555573>
- [9] Wu, Y. és Rooij, B. (2019). Compliance dynamism: Capturing the polynormative and situational nature of business responses to law. *Journal of Business Ethics*, 168(3), 579–591. <https://doi.org/10.1007/s10551-019-04234-4>
- [10] Silverman, M. (2008). *Compliance management for public, private, and nonprofit organizations*. McGraw Hill.
- [11] Suyunov, D. K. (2021). Scientific foundation for implementation of the compliance control system at corporate enterprises. *The American Journal of Management and Economics Innovations*, 3(6), 138–145. <https://doi.org/10.37547/tajmei/Volume03Issue06-21>
- [12] Statista. (é. n.). *Estimated amount of data created on the internet in one minute*. <https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet-in-one-minute/>
- [13] Srinivasan, R. és Zielinska, A. (2020). *Data at the edge: Managing and activating information in a distributed world*. State of the Edge; Seagate Technology. <https://www.stateoftheedge.com>
- [14] Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. és Byers, A. H. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute.
- [15] Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. SAGE Publications.
- [16] Norori, N., Alborno, D. és McBride, V. (2025). *Data and AI for science: Key considerations*. International Science Council. <https://doi.org/10.24948/2025.11>
- [17] Shameli-Sendi, A., Aghababaei-Barzegar, R. és Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 57, 14–30. <https://doi.org/10.1016/j.cose.2015.11.001>
- [18] ISO/IEC 22989:2022 (en), Information technology - Artificial intelligence - Artificial intelligence concepts and terminology; <https://www.iso.org/obp/ui/#iso:std:iso-iec:22989:ed-1:v1:en>.

- [19] Statista. (2023). Artificial intelligence market size. <https://www.statista.com/statistics/1365145/artificial-intelligence-market-size/>
- [20] Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age Work, Progress, and Prosperity in a Time of Brilliant Technologies*. W. W. Norton. <https://wwnorton.com/books/the-second-machine-age>
- [21] M.Raj and R. Seamans, “Primer on artificial intelligence and robotics,” *J. Organ. Des.*, vol. 8, no. 11, pp. 1–14, 2019. <https://doi.org/10.1186/s41469-019-0050-0>
- [22] Riemann, U. és Ochs, T. (2025). *Machine learning get ready to measure the value for supply chain management: Understanding the value of machine learning in the context of business processes*. https://doi.org/10.1007/978-3-031-92184-1_7
- [23] Furman, J. (2018). A mesterséges intelligencia és a gazdaság. NBER Working Paper No. 24689. https://www.nber.org/system/files/working_papers/w24689/w24689.pdf
- [24] Marković, M. és Soleša, D. (2025). Security and data protection in artificial intelligence. *Journal of Process Management New Technologies*, 13(1–2), 113–123. <https://doi.org/10.5937/jpmnt13-58872>
- [25] Wang, R. Y. és Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems*, 12(4), 5–33. <https://doi.org/10.1080/07421222.1996.11518099>
- [26] Anderson, R. (2008). *Security engineering: A guide to building dependable distributed systems*. Wiley.
- [27] Von Solms, R. és Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- [28] High-Level Expert Group on AI (2019). Ethics guidelines for trustworthy AI. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
- [29] Agrawal, A., Gans, J., & Goldfarb, A. (Eds.). (2019). *Economics of artificial intelligence: Agenda*. University of Chicago Press. <https://www.nber.org/books-and-chapters/economics-artificial-intelligence-agenda>
- [30] Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. Houghton Mifflin Harcourt. <https://dl.acm.org/doi/10.5555/2588165>
- [31] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>
- [32] Niskanen, T., Sipola, T. és Väänänen, O. (2023). *Latest trends in artificial intelligence technology: A scoping review*. JAMK University of Applied Sciences. <https://doi.org/10.48550/arXiv.2305.04532>
- [33] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., & al., e. (2014). Generative adversarial nets. *NeurIPS*. <https://papers.neurips.cc/paper/5423-generative-adversarial-nets.pdf>
- [34] McKinsey. (2019) Driving impact at scale from automation and AI., <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/driving-impact-at-scale-from-automation-and-ai>
- [35] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2). https://doi.org/10.1177/2053951716679679_1
- [36] Etzioni, A., Etzioni, O. (2017). Incorporating ethics into artificial intelligence. *The Journal of Ethics*, 21(4), 403–418. https://doi.org/10.1007/978-3-319-69623-2_15
- [37] Hodges, C. (2015). *Law and corporate behaviour: Integrating theories of regulation, enforcement, compliance and ethics*. Bloomsbury Publishing.
- [38] Painter, R. W. (2017). *Ethics and compliance: The corporate guide*. Oxford University Press.

- [39] Thompson, R. B. (2020). *Corporate governance after the financial crisis*. Oxford University Press.
- [40] McKinsey. (2023). The state of AI in 2023: Generative AIs breakout year. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year>
- [41] Raji, I. D., Smart, A., White, R. N., et al. (2020). Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. 2020. <https://doi.org/10.1145/3351095.3372873>
- [42] McKinsey. (2021). The state of AI in 2021. <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/Global%20survey%20The%20state%20of%20AI%20in%2021/Global-survey-The-state-of-AI-in-2021.pdf>
- [43] Danielsson, J., Macrae, R. és Uthemann, A. (2019). Artificial intelligence and systemic risk. *SSRN Electronic Journal*, 1–9. <https://doi.org/10.2139/ssrn.3410948>
- [44] Cao, L. (2022). AI in finance: Challenges, techniques, and opportunities. *ACM Computing Surveys*, 55(3), 1–38. <https://doi.org/10.1145/3502289>
- [45] Nichols, P. M. (2025). Does compliance with the global anticorruption regime require the use of artificial intelligence? *American Business Law Journal*, 62(3). <https://doi.org/10.1111/ablj.70000>
- [46] Pandya, U. (2025). Enhancing cloud security and compliance through artificial intelligence: A conceptual framework. *International Journal of Emerging Trends in Computer Science and Information Technology*. <https://doi.org/10.56472/ICCSAIML25-135>
- [47] Association of Certified Fraud Examiners: Occupational Fraud 2022: A Report to the Nations; <https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf>
- [48] Becker, S. és Mtsai. (2020). Continuous compliance. *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*, 1–12. <https://doi.org/10.1145/3324884.3416593>
- [49] López, H. A. és Hildebrandt, T. T. (2024). *Three decades of formal methods in business process compliance: A systematic literature review*. arXiv. <https://arxiv.org/abs/2410.10906>
- [50] Rinderle-Ma, S., Winter, K. és Benzin, J.-V. (2022). *Predictive compliance monitoring in process-aware information systems: State of the art, functionalities, research directions*. arXiv. <https://arxiv.org/abs/2205.05446>
- [51] Sharpe, L. K., Fong, P. S. és Sevia, R. E. (1998). Managing standards compliance. *IEEE Transactions on Software Engineering*, 24(6), 471–484. <https://doi.org/10.1109/32.824413>
- [52] Floridi, L. (2021). *The ethics of artificial intelligence*. Oxford University Press.
- [53] Európai Bizottság. (2017). Beruházás az intelligens, innovatív és fenntartható iparba: Megújult uniós iparpolitikai stratégia (COM/2017/0479 final). <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52017DC0479>
- [54] Európai Parlament. (2017). Jelentés a robotika polgári jogi szabályairól szóló bizottsági ajánlásokkal (2015/2103(INL)). <https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017IP0051>
- [55] Európai Tanács. (2017). Az Európai Tanács ülésének következtetései (EUCO 14/17). <https://www.consilium.europa.eu/media/21607/19-euco-final-conclusions-hu.pdf>
- [56] Európai Bizottság. (2018). EU Nyilatkozat a mesterséges intelligenciával kapcsolatos együttműködésről. <https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence>

- [57] Európai Bizottság. (2018). A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK A közös európai adattér kialakítása felé <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>)
- [58] Európai Bizottság. (2018). Az Európai Parlament és a Tanács rendelete a Digitális Európa program létrehozásáról a 2021-2027-es időszakra (COM(2018) 434 final, 2018/0227(COD)). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN>
- [59] Európai Parlament. (2019). Mesterséges intelligencia: Következtetések a mesterséges intelligenciával kapcsolatos összehangolt tervről (6177/19). <https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf>
- [60] Európai Bizottság. (2020). Fehér Könyv a mesterséges intelligenciáról: Az európai megközelítés a kiválóság és a bizalom érdekében. <https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:52020DC0065>
- [61] Európai Parlament és Tanács. (2024). Az Európai Parlament és a Tanács 2024. június 13-i (EU) 2024/1689 számú rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 számú rendeletek, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 számú irányelvek módosításáról (a mesterséges intelligenciáról szóló rendelet). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- [62] Európai Bizottság. (2025). *A mesterséges intelligencia általános célú gyakorlati kódexe*. <https://digital-strategy.ec.europa.eu/hu/policies/contents-code-gpai>
- [63] Deming, W. E. (1986). *Out of the crisis*. MIT Press.
- [64] Hammer, M., Champy, J. (1993). *Reengineering the corporation: A manifesto for business revolution*. Harper Business.
- [65] Nizza, R. (2024). Assessing the impact of the EU AI Act on innovation: A multi-model analysis. Northwestern Pritzker School of Law. https://www.law.northwestern.edu/research-faculty/clbe/events/standardization/documents/nizza_assessing_impact_ai_act_innovation.pdf
- [66] Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.
- [67] Veale, M. és Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law & Security Review*, 43, 105622. <https://doi.org/10.1016/j.clsr.2021.105622>
- [68] Calo, R. (2017). Artificial Intelligence Policy: A Primer and Roadmap. SSRN <https://ssrn.com/abstract=3015350>, <http://dx.doi.org/10.2139/ssrn.3015350>
- [69] van Rooij, B. és Sokol, D. D. (szerk.). (2021). *The Cambridge handbook of compliance*. Cambridge University Press. <https://doi.org/10.1017/9781108759458>
- [70] OECD. (2022) OECD Framework for the Classification of AI systems. (OECD Digital Economy Papers, No. 323). OECD Publishing. <https://doi.org/10.1787/cb6d9eca-en>
- [71] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>
- [72] Talaseela, R. K. (2025). Real-time compliance and exception handling via artificial intelligence. *Journal of Information Systems Engineering and Management*, 10(58s). <https://www.jisem-journal.com/>
- [73] Gösswein, G.: Mediation als Weg aus dem Compliance-Dilemma. *Die Mediation* (2) 2017. Magyar nyelvű fordítás: A mediáció mint a compliance dilemmából kivezető út (ford.: Csemáné Váradi E. – Jacsó J.), AKV Európai Szemle 1. (2017). pp. 122–127.

- [74] Balogh M.: A munkaügyi compliance audit, Wolters Kluwer, Budapest, 2015. pp. 15.
- [75] Bock, D.: Strafrechtliche Aspekte der Compliance-Diskussion – § 130 OWiG als zentrale Norm der Criminal Compliance, ZIS, 2. (2009). pp. 293.
- [76] Rotsch, T.: 4. Compliance. In ACHENBACH, H., RANSIEK, A.: Handbuch Wirtschaftsstrafrecht. 3. kiad., C. F. Müller, Heidelberg, 2012. pp. 47.
- [77] Ambrus, I., Mezei K., Molnár E.: Magyarázat a compliance jogszabályairól I., Általános és büntetőjogi compliance, Wolters Kluwer, Budapest, 2021 pp. 22.
- [78] Antal, T. és Számadó, R. (2025). A hazai és a nemzetközi szakirodalomban használatos compliance fogalmának vizsgálata bibliometriai elemzéssel: Kísérlet az újradefiniálására. Hadmérnök, 20 (2), 161–187. <https://doi.org/10.32567/hm.2025.2.10>
- [79] Pritchard, A. (1969). Statistical bibliography or bibliometrics. Journal of Documentation, 25(4), 348–349. <https://doi.org/10.1108/eb026482>
- [80] Otlet, P. (1934). Traité de documentation: Le livre sur le livre, théorie et pratique. Edition Mundaneum.
- [81] Garfield, E. (1955). Citation indexes for science: A new dimension in documentation through association of ideas. Science, 122(3159), 108–111. <https://doi.org/10.1126/science.122.3159.108>
- [82] van Eck, N. J., és Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2), 523–538. <https://doi.org/10.1007/s11192-009-0146-3>
- [83] Allam, Z. és Dhunny, Z. A. (2019). On big data, artificial intelligence and smart cities. Cities, 89, 80–91. <https://doi.org/10.1016/j.cities.2019.01.032>
- [84] Li, J., Greenwood, D. és Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. Automation in Construction, 102, 288–307. <https://doi.org/10.1016/j.autcon.2019.02.005>
- [85] Tandon, A., Dhir, A., Islam, A. K. M. N. és Mantymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, 103290. <https://doi.org/10.1016/j.compind.2020.103290>
- [86] Cram, W. A., D’Arcy, J. és Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43 (2), 525–554. <https://doi.org/10.25300/MISQ/2019/43.2.09>
- [87] Bernal Bernabe, J., Luis Canovas, J., Hernandez-Ramos, J. L., Torres Moreno, R. és Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7, 164908–164940. <https://doi.org/10.1109/ACCESS.2019.2950872>
- [88] Majumdar, A., Shaw, M. és Sinha, S. K. (2020). COVID-19 debunks the myth of socially sustainable supply chain: A case of the clothing industry in South Asian countries. Sustainable Production and Consumption, 24, 150–155. <https://doi.org/10.1016/j.spc.2020.07.001>
- [89] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J. és Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, 101653. <https://doi.org/10.1016/j.cose.2019.101653>
- [90] Mackey, T. K., Kuo, T.-T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., Obbad, K., Barkovich, R. és Palombini, M. (2019). Fit-for-purpose? – challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine, 17 (1), 68. <https://doi.org/10.1186/s12916-019-1296-7>
- [91] D’Arcy, J. és Lowry, P. B. (2019). Cognitive-affective drivers of employees’ daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, 29 (1), 43–69. <https://doi.org/10.1111/isj.12173>

- [92] Attaran, M. (2020). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, 15 (1), 70–83. <https://doi.org/10.1080/20479700.2020.1843887>
- [93] Giuditta, T., Hilde, V. M., Alessandra, P., Annick, S., Arthi, A., Artur, Z., ... Justine, G. (2024). Supporting measures to improve biosecurity compliance in poultry farms: the NetPoulSafe project. In: 8th International conference on poultry intestinal health, 108–109.
- [94] Bálint, F. (2023). Anti-money laundering with a special focus on the cyber security threats and vulnerabilities. *National security review: Periodical of the military national security service*, 2023(2), 144–157.
- [95] Delpont, M., Salazar, L. G., Dewulf, J., Zbikowski, A., Szeleszczuk, P., Dufay-Lefort, A.-C., ... Paul, M. C. (2023). Monitoring biosecurity in poultry production: an overview of databases reporting biosecurity compliance from seven European countries. *Frontiers in veterinary science*, 10. <http://doi.org/10.3389/fvets.2023.1231377>
- [96] Dunay, P. (2020). Arms Control Arrangements under the Aegis of the OSCE: Is There a Better Way to Handle Compliance? In: *Times of Eroding Cooperative Security: How to Save Conventional Arms Control in Europe*, 51–69.
- [97] Bicaku, A., Schmittner, C., Rottmann, P., Tauber, M., & Delsing, J. (2019). Security Safety and Organizational Standard Compliance in Cyber Physical Systems. *Infocommunications Journal*, 11(1), 2–9. <http://doi.org/10.36244/ICJ.2019.1.1>
- [98] Barta, G. (2018). Challenges in the compliance with the General Data Protection Regulation: Anonymization of personal information and related information security concerns. In *Knowledge – economy – society. business, finance and technology as protection and support for society*, 115–121.
- [99] Dunay, P. (2000). The CFE Compliance record a decade after treaty signature. *S + F: Sicherheit und frieden: security and peace*, 18(4), 327–333.
- [100] Antal, T. és Számadó, R. (2026). Design and evaluation of a compliance management framework for business operations: A system engineering perspective. *Journal of Engineering Management and Systems Engineering*, 5 (2), 120–136. <https://doi.org/10.56578/jemse050201>
- [101] Dhal, S. B., és Kar, D. (2025). Leveraging artificial intelligence and advanced food processing techniques for enhanced food safety, quality, and security: A comprehensive review. *Food Control*, 155, 110024. <https://doi.org/10.1016/j.foodcont.2024.110024>
- [102] Chen, D., et al. (2025). Optimizing the compliance third-party supervision workflow of involved enterprises using artificial intelligence ant colony algorithm. *Scientific Reports*, 15, 12202. <https://doi.org/10.1038/s41598-025-97115-y>
- [103] Ali, S., Razzaque, M. A., Yousaf, M., és Shan, A. (2025). Cloud security automation through symmetry: Threat detection and response. *Symmetry*, 17(6), 859. <https://doi.org/10.3390/sym17060859>
- [104] Filipović, A. M., Bralić, V., és Tripalo, S. (2025). Automated analysis of SSL/TLS certificates and network communication security in compliance with the Cybersecurity Act. *Crisis Management Days*. <https://ojs.vvg.hr/index.php/DKU/article/view/760>
- [105] Isazade, A., Malik, A., & Alshawki, M. B. (2025). Blockchain-enabled GDPR compliance enforcement for IIoT data access. *Journal of Cybersecurity and Privacy*, 5(4), 84. <https://doi.org/10.3390/jcp5040084>
- [106] Jacsó, J. (2019). A pénzmosás compliance a hazai és európai dimenzióban a társadalmi innováció tükrében. *Miskolci Jogi Szemle*, 2(1), 397–410.
- [107] Institute of Internal Auditors. (2020). THE IIA'S THREE LINES MODEL. An update of the Three Lines of Defense

- [108] Financial Markets Standards Board. (2020). The 3 Lines Model: A lens on risk management frameworks. <https://fmsb.com/publication/the-3-lines-model-a-lens-on-risk-management-frameworks/>
- [109] Eulerich, M. (2022). The new three lines model... Corporate Ownership & Control, 18(2), 183–191. <https://doi.org/10.22495/cocv18i2art15>
- [110] Magyar Nemzeti Bank. (2022. augusztus 11.). 12/2022. (VIII.11.) számú ajánlása. <https://www.mnb.hu/letoltes/12-2022-belso-vedelmi-vonalak-ajanlas.pdf>
- [111] Alrawashdeh, N., Jawad, M. A., Masoud, M., Al-Afeef, M. A., Al-Smadi, R. W., és Al Ibbini, O. A. (2025). Intelligent finance: Exploring the convergence of AI and fintech. In *Studies in systems, decision and control* (pp. 695–708). Springer International Publishing. https://doi.org/10.1007/978-3-031-90271-0_49
- [112] Salama, R., Cacciagrano, D., Al-Turjman, F. (2025). Connecting AI and Blockchain to Improve Security of Financial Services. In: Barolli, L. (eds) *Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2024. Lecture Notes on Data Engineering and Communications Technologies*, vol 232. Springer, Cham. https://doi.org/10.1007/978-3-031-76462-2_7
- [113] Magyar Nemzeti Bank. (2022). A belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról (Ajánlás No. 12/2022. (VIII.11.)). <https://www.mnb.hu/letoltes/12-2022-belso-vedelmi-vonalak-ajanlas.pdf>
- [114] George, B. és Vondra, A. (2023). Building a culture of compliance in life sciences organizations. *Journal of Commercial Biotechnology*, 28(1), 1–8. <https://doi.org/10.5912/jcb1005>
- [115] Borbás, Gy., Leitner, Gy., Bogsch, E. és Brázay, A. (2012). A gyógyszer-kommunikáció etikai kódexe. Magyarországi Gyógyszergyártók Országos Szövetsége.
- [116] Miftari, C. S., és Aliu, A. (2025). Designing a tailored ERP system with localized architecture for North Macedonian enterprises. 1991–1996. <https://doi.org/10.1109/mipro65660.2025.11131743>
- [117] Shah, R., Shah, S., és Pathak, P. (2025). Metaverse work culture: The emergence of virtual-first companies and HR's role. *Strategic HR Review*, 24(5), 195–200. <https://doi.org/10.1108/shr-03-2025-0029>
- [118] Singh, B., és Dutta, P. K. (2025). Cloud native engineering for AI-driven ERP systems: Enhancing security, compliance and data privacy. In *Advances in computers* (o. 439–463). Elsevier BV. <https://doi.org/10.1016/bs.adcom.2025.06.009>
- [119] Singh, K. R., Khanna, M., és Singh, R. (2026). The role of digital twin technology in sustainable smart cities. In *Elsevier eBooks* (o. 233–249). Elsevier BV. <https://doi.org/10.1016/b978-0-443-27388-9.00007-6>
- [120] Soares B. R. Filho, W., de Sousa, L. A. N., Pinto, H. A., Fontes, R. S., Caldeira Silva, G. J. P., Martins Fernandes, F. B., Barbalho, I. M. P., de Moraes, A. H. F., Arrais Júnior, E., de Oliveira Barreto, T., Teixeira, C., Henriques, J., Machado, G. M., Valentim, J. L. R. S., Coutinho, K. D., és Valentim, R. A. M. (2026). Brazilian national telediagnosis platform: A data report for scientific research and public health improvement. *Frontiers in Digital Health*, 8, 1766606. <https://doi.org/10.3389/fdgth.2026.1766606>
- [121] Grant, O. és Agoro, H. (2021). Trends in network compliance and regulatory challenges. ResearchGate. https://www.researchgate.net/publication/389674261_Trends_in_Network_Compliance_and_Regulatory_Challenges
- [122] Song, X., Liu, X., Yang, X., Si, C., Zuo, X., He, J., és Cui, Y. (2025). Strategizing data compliance in intelligent healthcare: A four-step solution. *Chinese Medical Journal*, 138(10), 1254–1256. <https://doi.org/10.1097/cm9.0000000000003434>

- [123] АНАНЬЕВА, О., és ГОНЧАР, В. (2026). Analysis of modern AI technologies in business: Algorithms and optimization methods, advantages and risks of application. *Scientific Notes of the University KROK*, 88–94. <https://doi.org/10.31732/2663-2209-2026-81-88-94>
- [124] Bârsan-Moigrădean, M. A. (2025). Legal aspects of the Lisbon Treaty on the European. *Cluj University Journal Interdisciplinary Social Sciences and Humanities*, 3(3-4), 7–20. <https://doi.org/10.61846/cuji-ssh.2025.3-4.02>
- [125] Ebrahim, A. (2025). *Enhancing domestic revenue mobilization in a reformed international financial architecture: Strategies for developing countries in a globalized tax landscape* [Jelentés]. <https://doi.org/10.35188/unu-wider/usuc9887>
- [126] Khezam, Y. B., Gamarnik, I. A., és Gendon, A. L. (2026). The use of artificial intelligence technologies for regulatory risk monitoring in the internal audit system. *Ekonomika i Upravlenie Problemy Resheniya*, 4/2(169), 200–207. <https://doi.org/10.36871/ek.up.p.r.2026.04.02.022>
- [127] Lakhamraju, M. V. (2025). The strategic role of workday payroll in addressing enterprise challenges. 2(1), 3–6. <https://doi.org/10.69517/cser.2025.02.01.0002>
- [128] Vankayalapati, R. K. (2025). Security and compliance in hybrid cloud models. https://doi.org/10.70593/978-81-984306-5-6_8
- [129] Eurostat. (2023). Use of artificial intelligence in enterprises. Európai Bizottság. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises
- [130] Európai Bizottság. (2022). Digital Economy and Society Index (DESI) 2022: Hungary. <https://digital-strategy.ec.europa.eu/en/policies/desi-hungary>
- [131] Európai Bizottság. (2023). 2023. évi jelentés a digitális évtized helyzetéről: Magyarország. <https://digital-strategy.ec.europa.eu/hu/library/2023-report-state-digital-decade-hungary>
- [132] Cahn, E. S. (2018). The King Midas monoculture. *Tikkun*, 33(1), 36–41. <https://doi.org/10.1215/08879982-6817889>
- [133] Andorka, R. (2006). Bevezetés a szociológiába. Osiris.
- [134] Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *Journal of Common Market Studies*. Advance online publication. <https://doi.org/10.1111/jcms.13654>
- [135] Frederica, D., & Murwaningsari, E. (2021). The effect of the use of artificial intelligence and operational risk management on banking performance with the implementation of regulation as a moderation variable. *DeReMa (Development Research of Management)*, 20(1). <https://doi.org/10.1877/degres.v20i1.50>
- [136] Hutchinson, J., Stilinovic, M., és Gray, J. (2024). Data sovereignty: The next frontier for internet policy? *Policy & Internet*. <https://doi.org/10.1002/poi3.386>
- [137] Ijaiya, H., & Adeniyi, I. A. (2024). AI and personal data privacy in the U.S: Balancing customer convenience with privacy compliance. *ABUAD Law Journal*, 12(1). <https://doi.org/10.53982/alj.2024.1201.03-j>
- [138] Li, Y., Wang, S., & Khaskheli, M. B. (2024). Integrating artificial intelligence into service innovation, business development, and legal compliance: Insights from the Hainan Free Trade Port era. *Systems*, 12(11), 463. <https://doi.org/10.3390/systems12110463>
- [139] Maitra, R., & Shrivastav, A. (2024). The data advantage: Artificial intelligence in ophthalmology. *Delhi Journal of Ophthalmology*. https://doi.org/10.4103/dljo.dljo_178_24
- [140] McKenna, B., Cai, W., és Tuunanen, T. (2024). Transforming to a sustainable visitor economy with information systems. *Information Systems Journal*. <https://doi.org/10.1111/isj.12573>

- [141] Mokale, M. (2021). Navigating global data privacy regulations: A guide for telecom operators. *International Journal for Multidisciplinary Research*, 3(4). <https://doi.org/10.36948/ijfmr.2021.v03i04.39051>
- [142] Nanumura, U., & Kumara, I. N. (2024). Including GRC principles in IoT security: A comparison of current approaches and future prospects. *International Journal of Innovative Science and Research Technology (IJISRT)*, 9(3). <https://doi.org/10.38124/ijisrt/ijisrt24mar227>
- [143] Rajamäki, J., Jarzowski, D., Kucera, J., Nyman, V., Pura, I., Virtanen, J., Herlevi, M., & Karlsson, L. (2024). Implications of GDPR and NIS2 for cyber threat intelligence exchange in hospitals. *WSEAS Transactions on Computers*, 23, 1. <https://doi.org/10.37394/23205.2024.23.1>
- [144] Shchavinsky, Y., Muzhanova, T., Yakymenko, Y., & Zaporozhchenko, M. (2023). Application of artificial intelligence for improving situational training of cybersecurity specialists. *Information Technologies and Learning Tools*, 97(5). <https://doi.org/10.33407/itlt.v97i5.5424>
- [145] Zahid, A., & Sharma, R. (2023). Personalized health care in a data-driven era: A post-COVID-19 retrospective. *Mayo Clinic Proceedings: Digital Health*, 1(2). <https://doi.org/10.1016/j.mcpdig.2023.04.002>
- [146] Berwer, R. K., Indora, S., Atal, D. K., & Yadav, V. (2024). Blockchain technology for Industry 4.0. In *Blockchain technology and applications*. <https://doi.org/10.1002/9781394216147.ch6>
- [147] Dimitrov, W. (2020). Analysis of the need for cyber security components in the study of advanced technologies. In *INTED2020 Proceedings*. <https://doi.org/10.21125/inted.2020.1423>
- [148] Dorairajan, V. (2024). Cybersecurity and organisational performance – the interplay. *ARPHA Conference Abstracts*. <https://doi.org/10.3897/aca.7.e129255>
- [149] Herath, H.M.S.S., Herath, H.M.K.K.M.B., Madhusanka, B.G.D.A., Guruge, L.G.P.K. (2024). Data Protection Challenges in the Processing of Sensitive Data. In: Hewage, C., Yasakethu, L., Jayakody, D.N.K. (eds) *Data Protection*. Springer, Cham. (pp.155-179). https://doi.org/10.1007/978-3-031-76473-8_8
- [150] Kazi, M. R., P., S., Buvanewari, R., és Kumar, S. S. (2024). *Modern commerce*. <https://doi.org/10.61909/amkedtb112437>
- [151] Maguluri, K. K. (2025). Foundations of artificial intelligence in healthcare IT: An overview of innovation. In *How Artificial Intelligence is Transforming Healthcare IT: Applications in Diagnostics, Treatment Planning, and Patient Monitoring* (pp. 1-15). Deep Science Publishing. https://doi.org/10.70593/978-81-984306-1-8_1
- [152] Maguluri, K. K. (2025). Natural language processing in healthcare: Unlocking insights from clinical data. In *How Artificial Intelligence is Transforming Healthcare IT: Applications in Diagnostics, Treatment Planning, and Patient Monitoring* (pp. 72-88). Deep Science Publishing. https://doi.org/10.70593/978-81-984306-1-8_5
- [153] Rane, N. L., Paramesha, M., Rane, J., & Mallick, S. K. (2024). Policies and regulations of artificial intelligence in healthcare, finance, agriculture, manufacturing, retail, energy, and transportation industry. In N. L. Rane (Ed.), *Artificial Intelligence and Industry in Society 5.0* (pp. 67-81). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-1-2_4
- [154] Sargiotis, D. (2024). Future Trends in Data Governance: Preparing for Tomorrow. In: *Data Governance*. (pp. 365-390) Springer, Cham. https://doi.org/10.1007/978-3-031-67268-2_12

8 A tézispontokhoz kapcsolódó tudományos közlemények

H2; H3 Antal, T., & Számadó, R. (2026). Design and Evaluation of a Compliance Management Framework for Business Operations: A System Engineering Perspective. JOURNAL OF ENGINEERING MANAGEMENT AND SYSTEMS ENGINEERING, 5(2), 120–136. <http://doi.org/10.56578/jemse050201>

H2; H3 Antal, T., & Számadó, R. (2025). As Many Organizations, as Many Compliance Solutions—Enforcement of Special Protection in Practice. In The Impact of the Energy Dependency on Critical Infrastructure Protection (pp. 103–111). http://doi.org/10.1007/978-3-031-78544-3_8

H1 Antal, T., & Számadó, R. (2025). From theory to practice: analysis of artificial intelligence regulation in the European Union – recommendation on general terms and conditions. BIZTONSÁGTUDOMÁNYI SZEMLE, 7(4), 167–176. <http://doi.org/10.12700/btsz.2025.7.4.167>

H1 Antal, T., & Számadó, R. (2025). A hazai és a nemzetközi szakirodalomban használatos compliance fogalmának vizsgálata bibliometriai elemzéssel. HADMÉRNÖK, 20(2), 161–187. <http://doi.org/10.32567/hm.2025.2.10>

H2; H3 Tímea, A., & Róza, S. (2025). A snapshot of the emergence of compliance and Artificial Intelligence – results of an online survey of Hungarian companies. ANNALS OF FACULTY OF ENGINEERING HUNEDOARA: INTERNATIONAL JOURNAL OF ENGINEERING, 23(2), 173–180.

H1 Tímea, A. (2023). First Steps - Compliance and Artificial Intelligence. In 16th Annual International Conference on Economics and Business: Challenges in the Carpathian Basin : Towards a new sustainability? (pp. 149–156).

H1 Tímea, A. (2023). Plan-Do-Check-Act In the Context of Compliance. In 16th Annual International Conference on Economics and Business: Challenges in the Carpathian Basin : Towards a new sustainability? (pp. 157–166).