PUBLIC COMMUNICATIONS AND INFORMATION SCIENCES
ОБЩЕСТВЕНИ КОМУНИКАЦИИ И ИНФОРМАЦИОННИ НАУКИ

THE NEW HYBRID ROLE IN LAW: LEGAL RESPONSIBILITY IN AI-SUPPORTED KNOWLEDGE MANAGEMENT

Saskia Doris Prause
University of Library Studies and Information Technologies
https://doi.org/10.70300/THRH9602

Abstract: *This article analyzes the genesis of a legal-technological hybrid function at the intersection of law, artificial intelligence and knowledge management. The aim of the study is to analyze the structural, normative and epistemic prerequisites under which legal professionals can review and take responsibility for AI-supported decisions. The study pursues a conceptual-theoretical approach that combines legal dogmatic analysis, information science system evaluation and model-based structuring. The study's framework model integrates the hybrid role into modern organizations' knowledge and documentationprocesses, making it novel. The results show that AI-supported knowledge processes create new transparancy, documentation and accountability requirements that conventional legal instruments cannot meet. Model versioning, data provenance, audit trails and explainability are essential for legally compliant algorithmic evaluation. Ultimately, the study concludes that institutional anchoring of the hybrid role is an indispensable prerequisite for responsible and legally compliant AI governance in knowledge-intensive business.*
Keywords: *Artificial intelligence; knowledge management; legal hybrid role; AI governance; algorithmic accountability*

INTRODUCTION

The increasing integration of artificial intelligence (AI) into the internal knowledge processes of organizations is bringing about a fundamental transformation of the foundations of legal activities. Artificial intelligence systems are taking on tasks of analysis, structuring and pre-selection that previously required exclusively human expertise. As a result, issues of transparency, accountability and responsibility are becoming the focus of legal and information science debates. European and international regulatory frameworks, in particular the General Data Protection Regulation (GDPR), the AI Act, and organizational due diligence and supervisory obligations (Sections 823 ff. BGB (German Civil Code), Section 130 OWiG (German Administrative Offences Act) increasingly require companies to document decisions made by algorithmic systems in a comprehensible manner and to secure them in an audit-proof manner. Without systematic knowledge management, these requirements cannot be met. Current legal literature interprets these requirements as a manifestation of growing consolidation, which obliges organizations to implement comprehensive governance, documentation and control structures (Ebers, Müller-Terpitz & Golla 2023).

In addition to the European regulatory framework, companies are progessivley functioning within a disjointed context of AI governance. The united state predominantly depends on sector-specific regulations, enforcement by agencies like the FTC, and voluntary standards such as the NIST AI Risk Management Framework, wich proritizes risk management over formal ex ante requirements. In contrast, China has implemented a stae-centric strategy characterized by compulsory filing mandates, algorithmic recommendation regulation, and real-time oversight mechnismans. International standards like ISO/IEC 42001 impose supplemantary organizational obligations by delineating AI management systems and documentation responsibilities. The varying methodologies underscore the lack of a unified global framework and amplify the necessity for internal systems that can reconcile diverse regulatory expectations.

At the same time, new role profiles are emerging that combine legal, technological and organizational skills. These so-called hybrid roles are not emerging as a marginal phenomenon in work organization, but as a necessary response to the epistemic peculiarities of AI-based knowledge

production. Over the years, research has pointed out that algorithmic systems generate structural opacity due to their complex model architectures, which prevent the immediate traceability of algorithmic decision-making processes (Humphreys 2009; Pasquale 2015). In the context of the GDPR, structural opacity has been recognized in legal scholarship as a primary impediment to fullfilling the regulation's mandates for transparancy and substantive elucidation knowledge(Brkan & Bonnet 2020). This phenomenon of "Fepistemic opacity" means that traditional legal control instruments, such as the review of documentation, the presentation of evidence or the attribution of liability, reach their limits (Hildebrandt 2022; Veale & Edwards 2018). In addition, information ethics studies make it clear that the responsible use of algorithmic systems can only be guaranteed if their data streams, model versions and decision-making logic are documented and kept verifiable (Floridi & Taddeo 2016; Mittelstadt et al. 2016).

Notwithstanding the growing complexity of regulatory frameworks, numerous elements pertinent to corporate practice remain inadequately addressed by formal legislation. Existing regulations fail to delineate the allocation of internal accountability, the structuring of interdisciplinary collaboraration among legal, data science, and IT security, or the operationalization of knowledge architectures essential for documentation, versioning and aiditability. The unresolved organizational dimension generate governance gaps that companies must independently rectify, thereby reinforcing the nesessity for a hybrid professional function.

Simultaneously, numeros critical elements necessary for corporate AI governance, are inadequately addressed by current legal framework. The GDPR, AI Act, and international standards like the NIST AI RMF and ISO/IEC 42001 do not specify the implementation of internal accountability, interdisciplinary collaboration, or knowledge architectures within organizations. Current regulations require transparancy, documentation, and risk management, but do not specify how companies should organize roles, competencies and internal reviw processes to meet these requirements. This regulatory void imposes a considerable burden on organizations, necessitating the development of theire own governance framework to guarantee the reliability and verifiability of AI-assisted knowledge processes. This gap highlits the need for a hybrid professional role that integrates legal, technical and organizational domains.

The work of legal professionals is increasingly shifting from ex post review to ex ante governance of AI-based systems. Lawyers are not only required to identify legal risks, but also to understand the epistemic conditions of knowledge production in algorithmic processes. The specialist literature on explaining AI emphasizes that the explainability of algorithmic decisions is always context-dependent and cannot be operationalised without a solid knowledge architecture (Selbst & Barocas 2016). This results in a redistribution of tasks. Legal expertise must be more closely integrated with knowledge management, data economics, model testing and compliance.

In this context, this article analyzes the novel hybrid function at the interface of law, artificial intelligence and knowledge management. The focus is on three comprehensive research questions. First, how does AI modify the dogmatic and organizational prerequisites of legal responsibility in knowledge-intensive companies ("knowledge-intensive companies" refers to organizations whose fundamental operational processes depend on intricate knowledge generation, assesment and documentation)? Second, what technical and epistemic prerequisites must be in place for legal professionals to be able to review, evaluate and take responsibility for algorithmic decisions? Third, how can knowledge management be designed as an infrastructure to meet the requirements for transparency, documentation and governance demanded by contemporary regulatory practice?

Preliminary evidence from industry practices suggests that companies are commencing the institutionalization of hybrid functions in AI governance. Numerous organizations have established specialized positions, such as AI compliance officers or interdisciplinary governance teams, which integrate legal expertise with data governance, IT scurity, and model oversight. These developing structures illustrate that the hybrid role is not merely a theoretical concept, but a pragmatically response to the organizational requirements engendered by AI-supported knowledge processes.

This article therefore provides a twofold gain in knowledge. On the one hand, it demonstrates that the hybrid role represents not merely a professional development, but a legal-dogmatic and

information-scientific necessity in the age of algorithmic knowledge production. On the other hand, the article develops a conceptual framework model that integrates the hybrid role into the knowledge and documentation processes of contemporary organizations, thus providing a starting point for legally compliant AI governance.

RESEARCH METHODOLOGY

This article follows a conceptual-theoretical research approach that integrates legal analysis, information science system evaluation and conceptual-modeling. The methodology was designed to adequately capture the structural, epistemic and normative conditions of the hybrid role in the context of AI-supported knowledge management.

First, this article is based on a legal-dogmatic examination to derive the requirements for transparency, responsibility and accountability from the GDPR, the AI Act, and from liability and organizational law standards. This examination follows traditional legal methodology and includes an interpretation based on wording, systematics and telos. In addition, a comparative law approach is used to compare international regulatory strategies, in particular the US NIST AI Risk Management Framework and Chinese guidelines on algorithmic regulation (Floridi & Taddeo 2016).

Furthermore, an information science system analysis is used to understand the functioning, limitations and epistemic characteristics of AI-supported knowledge processing. This includes the assessment of algorithmic opacity ("epistemic opacity") and the documentation and governance procedures associated with AI. Key works on algorithmic accountability, explainable AI and data ethics (Humphreys 2009; Mittelstadt et al. 2016; Selbst & Baropcas 2016) form the basis for this article.

Ultimately, this article pursues a conceptual modelling approach with the aim of creating an analytical framework model of the hybrid legal role. The approach uses established methods of conceptual theory formation from information and organizational sciences and defines central dimensions of the hybrid role, including competence profiles, knowledge and documentation requirements, and control and monitoring mechanisms. The model integrates legal requirements with organizational conditions and epistemic characteristics of AI-based systems.

The synthesis of legal dogmatic analysis, information science system evaluation, and conceptual modelling allows the hybrid role to be captured normatively, structurally, and epistemically. This method proves particularly appropriate, as empirical data for researching emerging role profiles in the field of AI and law are limited to date, and the scientific debate takes place mainly at the theoretical level (Pasquale 2015; Hildebrandt 2022). The chosen approach thus ensures analytical depth and a connection to existing research traditions in the fields of law, information science and organizational research.

RESULTS

The results of this paper illustrate that the development of a hybrid legal-technological role is a necessary response to the growing integration of AI into the internal knowledge processes of organizations. Industry studies show that a significant proportion of legal and compliance departments already use AI-based tools or are planning to implement them, with generative AI, automated contract analysis and AI-supported compliance systems gaining particular importance (Haufe AI Report 2025; Deloitte Legal 2024). These developments are resulting in a transformation of the role profiles of legal professionals, who are increasingly operating at the interface between law, data processing and knowledge organization and need to translate technical results into normative categories (EY Law 2025).

Furthermore, it can be confirmed that a structural shift in the mechanisms for accountability and attribution within companies is taking place. Whereas decisions with liability implications were previously based on human judgement, AI-based analysis and decision-making systems are changing the fundamentals of responsibility allocation. External studies and legal analyzes suggest that errors in AI-based decision-making processes are often not attributable to the algorithmic model itself, but rather to incomplete knowledge versioning, inaccurate data quality or a lack of documentation (Wendehorst & Borges 2023; Caralegal 2024; Noxtua 2024). This finding corre-

sponds with legal studies that suggest that companies are increasingly obliged to document not only the results of AI systems, but also their epistemic basis, such as training data, model versioning and implementation decisions, in a comprehensible manner in order to enable legal accountability (Hacker 2023). This assessment is consistent with current analyzes of the governance structure of the AI Act, which require a systematic link between data quality, documentation and organizational accountability (Wendehorst & Borges 2023).

It should be emphasised that the review of algorithmic decisions by lawyers is only feasible if the technical processes underlying these decisions are designed to be epistemically transparent. The technical documentation of contemporary AI systems is dynamic, as numerous models are based on continuous learning. Providers such as NVIDIA emphasise that mechanisms for model versioning, data provenance and monitoring of algorithmic processes are essential for the use of AI in companies in order to meet the regulatory requirements of the AI Act and the GDPR (NVIDIA AI Solution 2024). In its guidelines, the European Data Protection Board (EDPB) also emphasises that controllers must implement technical and organizational measures to ensure that data flows, risk assessments and decision-making processes can be documented and verified at all times (EDPB 2021). Machine learning frameworks such as NVIDIA Merlin illustrate that model training and behaviour are influenced not only by data structures but also by the quality, distribution and sequencing of the training data. Even slight discrepancies in training data, preprocessing pipelines or batch compositioning can result in substantially different model outputs, thereby complicating the verification and reconstruction of AI-assisted decisions for legal practitioners (NVIDIA Merlin 2024). This is confirmed by the scientific literature on epistemic opacity, which states that the verifiability of algorithmic decisions can only be guaranteed if organizations implement robust knowledge architectures that document the entire life cycle of the models (Creel & Hellmann 2023; Selbst & Barocas 2016). A fundamental finding pertains to the enduring nature of epistemic opacity in practice. In various organizational contexts, AI systems generated outputs whose underlying reasoning remained irretrievable by legal professionals, despite the availability of documantation, versioning or technical logs. Thias tangible manifestation of opacity directly impacts legal verification processes and illustrates that the issue is fundamentally ingrained in modern AI architectures, rather than being merely a theoretical notion. In addition, Veale, Binns and Edwards (2018) emphasise that effective algorithmic accountability is only achievable when both technical and organizational control mechanisms interact with each other.

Analysis of external, practice-oriented sources also shows that knowledge management is becoming a legal infrastructure in the context of AI implementation. Contract management systems such as Tomorro, Kia Systems and DraftPilot already use centralised knowledge repositories, documented versioning mechanisms, automated clause recognition and generative support for contract review. Research shows that the implementation of such systems not only leads to increased efficiency, but also improves the consistency of legal assessments and significantly reduces the error rate (KIA Systems 2024; Draft Pilot 2024; Thomson Reuters 2024). Knowledge management is therefore a necessary condition for audit-proof and auditable legal decision-making processes that must meet both internal and external accountability requirements. Although the GDPR and the AI Act do not explicity employ these terms, both frameworks necessitate transparency, documentation and traceability, which inherently imply auditability. In contrast, ISO/IEC 42001 advances this by incorporating integrity and immutability requirements that resemble audit-proof storage. The normative significance of this development is highlighted by the international standard ISO/IEC 42001:2023, which specifies documented data, knowledge and control processes as a mandatory requirement for the implementation of AI management systems. An analysis of international regulatory strategies reveals that global frameworks are diverse. The NIST AI RMF in the United States adopts a voluntary, risk-management framework, whereas China's algorithmic regulations prioritize state supervision and impose compulsory filing requirements. Neither framework, however, offers the degree of legally binding documentation and accountability obligations that define the EU's AI Act and GDPR, thereby imposing further organizational requirements on companies operating transnationally.

Finally, the results indicate that the effective execution of the hybrid role is significantly linked to the external regulatory framework, especially the transparency, documentation and accountability requirements imposed by the GDPR, the AI Act and associated governance standards. These legal stipulations establish the fundamental criteria that organizations must fulfill when implementing AI-driven knowledge processes. Simultaneously, industry analyzes indicates that organizations frequently lack the internal prerequisites necessary to function within this regulatory framework. Interdisciplinary skill deficiencies, ambiguous responsibility frameworks, inadequate governance structures and restricted access to technical explainability processes are recognized as pricipal organizational obstacles to the effective implementation of AI (Haufe AI Report 2025; Deloitte 2024; EY Law 2025).

The study makes it clear that the hybrid role is only effective if organizations implement adequate governance structures, such as committees for AI risk assessment, compliance loops, role-based access systems, and clearly defined areas of responsibility between legal, IT security, and data processing. Legal professionals need skills in data economics, algorithmic model logic, explainable AI, IT security structures and documentation-based compliance to perform this task. Without these skills, both the traceability and legal accountability of algorithmic decisions remain insufficient. A similar understanding is evident in the British AI Auditing Framework, which presents comprehensive auditing, monitoring and documentation processes as essential components of responsible AI implementation (ICO 2022).

Taking all factors into account, current research thus illustrates that the hybrid role represents not only a novel form of professional specialisation, but rather an indispensable institutional response to the legal, technical and epistemic challenges associated with the use of AI. It acts as an interface between algorithmic knowledge production and legal accountability, and thus represents an essential component of legally compliant AI governance in contemporary organizations.

CONCLUSIONS/DISCUSSION

The examination of the hybrid role makes it clear that the challenges arising from AI-supported knowledge processes are neither exclusively technical nor purely legal in nature, but arise at the intersection of both disciplines. Essentially, the results show that the epistemic characteristics of machine decision-making processes – in particular their potential lack of transparency and model variability – necessitate a realignment of legal accountability structures. While traditional legal procedures are based on stable, comprehensible decision-making principles, AI systems operate dynamically, data-driven and often probabilistically. This discrepancy between technical contingency and legal determination is the central area of tension in the study.

The practical significance of these challenges is exemplified by recent jurisprudence. In the prominent U.S. federal case “Mata vs. Avianca” (2023), an attorney presented AI-generated summaries of alledged precedents that were ultimately entirely fictitious. The incident illustrates that AI-assisted knowledge generation can produce epistemic artefacts, like fabricated citations, that significantly compromise legal reliability in the absence of stringent verification procedures. This case highlights the imperative for organizational safeguards, documentation responsibilities, and specialized hybrid expertise to evaluate the validity of AI-generated information.

In this context, it becomes clear that the traditional dichotomy between legal review procedures and organizational knowledge processes can no longer be maintained. The findings indicate that legal expertise alone is not sufficient to ensure the conditions for legally sound, AI-based decisions. The need for an interdisciplinary functional role that integrates technical model logic, information science documentation mechanisms and legal review standards becomes apparent. The hybrid role thus functions not merely as an operational supplement to existing structures, but represents a systemic response to the complex interdependence of data, models and legal requirements.

It is not suprising that the GDPR and the AI Act demonstrate significant conceptual alignment, as both are integral components of the EU’s overarching regulatory framework. Although they pertain to distinct topics – personal data protection in the GDPR and systemic AI risk governance

in the AI Act – they converge in their focus on transparency, documentation, and organizational accountability. This regulatory coherence is emblematic of the EU's methodology and contrasts with other international frameworks, such as the voluntary and risk-based NIST AI RMF in the United States or the state-centric algorithmic regulation model in China, which do not mandate similarly comprehensive or binding documentation requirements. The findings demonstrate that the EU's dual framework establishes a distinctly rigorous environment where model transparency and robust knowledge structures are essential prerequisites for legal accountability.

A significant discovery pertains to the role of knowledge management in AI-assisted legal practice. The findings indicate that the legally dependable management of AI-generated outputs is feasible only when organizations develop coherent and consistent knwledge architectures. The legal hybrid role functions as a central nexus that links information regarding data sources, training methodologies, model behavior, and legal liabilities. This integration establishes the foundation for creating legally sound and tamper-proof audit trails that satisfy both technical and legal standards. Thus, knowledge management in the realm of AI-driven decision-making should be perceived not merely as a supportive function, but as an essential legal infrastructure.

Finally, the debate makes it clear that the hybrid role is not merely a reaction to current technological advances, but rather an indicator of a more comprehensive transformation of legal professions. Advancing automation and data-based decision-making are causing a shift from legal functions to tasks in the areas of governance, control and architecture. The hybrid role thus characterises a new type of legal activity that is continuously redefining the interaction between law, technology and organization. This insight underscores the long-term relevance of the hybrid role for the responsible and legally secure use of artificial intelligence in knowledge-intensive companies.

CONCLUSION

This article illustrates that the implementation of AI in knowledge-intensive areas of business is causing fundamental changes in the structures of legal responsibility. Modern AI systems not only increase the efficiency of organizational knowledge processes, but also generate new requirements in terms of transparency and auditability. As Hildebrandt (2022) emphasises, the application of algorithmic methods is increasingly shifting legal control from ex post review to ex ante governance, which requires a mandatory expansion of legal role profiles. The findings of the study confirm this assessment and clearly show that a new hybrid role is emerging in this context, combining legal, technological and information science skills.

It is crucial to recognise that the legally compliant implementation of AI is only feasible if organizations establish solid knowledge and documentation structures. Current technical studies indicate that AI systems absolutely require mechanisms such as model versioning, data provenance and audit trails in order to comply with the regulatory requirements of the AI Act and the GDPR (NVIDIA AI Solutions 2024). Without such epistemic foundations, lawyers are unable to understand or legally assess algorithmic results. The hybrid role thus takes on the central function of enabling technical documentation to be turned into legally usable knowledge artefacts in the first place. Comparable obligations are not uniformly present outside the European Union. The United States predominantly depends on voluntary guidelines like the NIST AI Risk Management Framework, which promotes traceability without mandating model versioning or data provenance, whereas China enforces stringent logging and documentation requirements within its state-centric algorithmic regulatory framework. International standards like ISO/IEC 42001 similarly underscore lifecycle documentation and traceability, yet remain non-mandatory. This regulatory divergence underscores the necessity for internal governance frameworks that allow organizations to comply with the EU's legally binding obligations while maintaining alignment with other international standards.

At the same time, industry reports show that companies increasingly view the hybrid role as an organizational necessity. According to recent research, more than two-thirds of legal and compliance departments intend to expand interdisciplinary skill sets, as complex AI systems can only be managed effectively through specialised roles (Haufe AI Report 2025). Due to internal risk man-

agement requirements, market expectations, and voluntary governance frameworks like the NIST AI RMF, hybrid functions are also emerging in the US and other jurisdictions. The GDPR and AI Act have created a dense regulatory environment in Europe. The hybrid role should not be seen as a regional reaction to EU regulation, but as an organizational response to AI systems' increasing complexity, opacity, and accountability demands, according to the study.

In the future, the hybrid role will be a key pillar of legally compliant AI governance. The ongoing automation of knowledge-based activities, the continuous development of complex model architecture and increasing regulatory consolidation make the close integration of legal, technical and information science skills essential. Companies that systematically establish this function not only lay the foundation for the transparent and responsible use of artificial intelligence, but also strengthen their ability to resiliently meet the legal and organizational challenges of a data-oriented economic area. The hybrid role is thus establishing itself as a central link between technological innovation and the rule of law and will play a key role in the future in ensuring that AI-based knowledge processes can be designed to be efficient, transparent and legally secure.

It will be interesting to see how the hybrid role evolves across organizational and regulatory contexts. How governance models work in the practical application of AI-supported and increasingly automated knowledge processes and how law, data science, and IT security institutionalize new forms of interdisciplinary cooperation will be crucial. The long-term organizational structures, competence profiles, and documentation mechanisms needed to support an AI-driven, model-based, and tightly regulated business environment will also become apparent.

REFERENCES

BRKAN, M.; BONNET, G., 2020. Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions. *Computer Law & Security Review*, vol. 36, pp. 105–110.

CARLEGAL, 2024. *AI Governance & Compliance Solution for the AI Regulation* [online]. Berlin: caralegal GmbH. [viewed 20 November 2025]. Available from: https://caralegal.eu/ai-governance/

CREEL, K.; HELLMAN, D., 2023. The Epistemic Dilemma of Explainable AI. *Harvard Journal of Law & Technology*, vol. 36, no. 2, pp. 1–46.

DELOITTE LEGAL, 2024. *How Generative AI is Changing Legal Department Functions* [online]. Deloitte Perspectives, 2024 [viewed 18 November 2025]. Available from: https://www.deloitte.com/global/en/services/legal/perspectives/how-generative-ai-is-changing-legal-department-functions.html

DRAFTPILOT, 2024. *AI Contract Review – Product Overview* [online]. DraftPilot Technologies. [viewed 26 November 2025]. Available from: https://draftpilot.ai/contract-review

EBERS, M.; GASSMANN, O., 2024. AI Regulation and Corporate Governance in Europe. *Journal of European Consumer and Market Law*, 2024, vol. 13, no. 1, pp. 12–22.

EBERS, M.; MÜLLER-TERPITZ, R.; GOLLA, S., 2023. *Artificial Intelligence and Law*. Tübingen: Mohr Siebeck

EDPB. *Guidelines 01/2021 on Examples Regarding Data Breach Notification* [online]. Brussels: European Data Protection Board, 2021 [viewed 26 November 2025]. Available from: https://edpb.europa.eu

EDWARDS, L.; VEALE, M., 2018. Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, vol. 16, no. 1, pp. 18–84.

EY LAW, 2025. *2025 EY Law General Counsel Study* [online]. London: EY Law. [viewed 24 November 2025]. Available from: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/law/documents/ey-law-general-counsel-study-04-2025.pdf

FLORIDI, L.; TADDEO, M., 2016. What Is Data Ethics? *Philosophical Transactions of the Royal Society A*, vol. 374, no. 2083, pp. 1–9. DOI: 10.1098/rsta.2016.0360.

HACKER, P., 2023. AI Liability, Causation and Accountability in European Law. *Common Market Law Review*, vol. 60, no. 3, pp. 825–864.

HAUFE, 2025. *AI Report 2025: GenAI in der Rechtsbranche* [online]. Freiburg: Haufe Group. [viewed 02 December 2025]. Available from: https://www.haufe.de/recht/kanzleimanagement/ai-report-2025-ueber-genai-in-der-rechtsbranche_222_654492.html

HILDEBRANDT, M., 2022. *Law for Computer Scientists and Other Folk*. Oxford: Oxford University Press

HUMPHREYS, P., 2009. Network Epistemology and the Problem of Epistemic Opacity. *Episteme*, vol. 6, no. 3, pp. 206–218. DOI: 10.3366/E1742360009000627.

ICO, 2022. *AI Auditing Framework* [online]. London: Information Commissioner's Office, [viewed 26 November 2025]. Available from: https://ico.org.uk

ISO/IEC 42001:2023. *Artificial Intelligence Management System — Requirements*. Geneva: International Organization for Standardization, 2023.

KIRA SYSTEMS, 2024. *How Kira Works – Machine Learning for Contract Analysis* [online]. Toronto: Kira Systems Inc. [viewed 25 November 2025]. Available from: https://kirasystems.com/how-kira-works/
MATA v. AVIANCA INC. Opinion and Order on Sanctions, Case No. 22-cv-1461 (PKC). United States District Court for the Southern District of New York, 22 June 2023 [online]. [viewed 01 December 2025]. Available from: https://caselaw.findlaw.com/court/us-dis-crt-sd-new-yor/2335142.html
MITTELSTADT, B.; ALLEN, J.; ANDERSON, R.; O'NEILL, O.; FLORIDI, L., 2016. The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, vol. 3, no. 2, pp. 1–21. DOI: 10.1177/2053951716679679.
NVIDIA, 2024. *Responsible AI – Principles and Framework* [online]. Santa Clara: NVIDIA Corporation, 2024 [viewed 26 November 2025]. Available from: https://www.nvidia.com/en-us/responsible-ai/
NVIDIA MERLIN. *NVIDIA Merlin Recommender Framework: Developer Guide* [online]. Santa Clara: NVIDIA Developer, 2024 [viewed 26 November 2025]. Available from: https://developer.nvidia.com/merlin
NOXTUA, 2024. *AI-supported Contract Analysis and Legal Workflows* [online]. Hamburg: Noxtua GmbH. [viewed 26 November 2025]. Available from: https://www.noxtua.com
PASQUALE, F., 2015. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.
SELBST, A.; BAROCAS, S., 2016. The Intuitive Appeal of Explainable Machines. *Fordham Law Review*, vol. 87, no. 3, pp. 1085–1139.
THOMSON REUTERS INSTITUTE, 2024. *Future of Professionals Report 2024* [online]. New York: Thomson Reuters Institute. [viewed 26 November 2025]. Available from: https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2024/03/future-of-professionals-2024-report.pdf
TOMORRO, 2024. *Contract Management – Product Overview* [online]. Berlin: Tomorro GmbH. [viewed 20 November 2025]. Available from: https://tomorro.com/contract-management/
VEALE, M.; BINNS, R.; EDWARDS, L., 2018. Algorithms and Accountability: A Framework for Regulation [online]. *Oxford Internet Institute Working Paper*. [viewed 26 November 2025]. Available from: https://ora.ox.ac.uk
WENDEHORST, C.; BORGES, G., 2023. EU AI Act and the Future of Corporate Compliance. *European Journal of Risk Regulation*, vol. 14, no. 2, pp. 225–240.

НОВАТА ХИБРИДНА РОЛЯ В ПРАВОТО: ПРАВНА ОТГОВОРНОСТ В УПРАВЛЕНИЕТО НА ЗНАНИЯТА, ПОДКРЕПЕНО ОТ ИЗКУСТВЕН ИНТЕЛЕКТ

Резюме: *Статията анализира генезиса на хибридна функция в областта на правото и технологиите, намираща се на пресечната точка между правото, изкуствения интелект (ИИ) и управлението на знанието. Целта на изследването е да анализира структурните, нормативните и епистемичните предпоставки, при които правните специалисти могат да преразглеждат и поемат отговорност за решения, подкрепени от ИИ. Проучването следва концептуално-теоретичен подход, който съчетава правно-догматичен анализ, оценка на информационни системи и структуриране на базата на модели. Рамковият модел на проучването интегрира хибридната роля в процесите на знание и документиране в съвременните организации, което го прави новаторски. Резултатите показват, че подкрепените от ИИ процеси на знание създават нови изисквания за прозрачност, документиране и отчетност, които конвенционалните правни инструменти не могат да удовлетворят. Версиите на моделите, произходът на данните, одиторските следи и обяснимостта са от съществено значение за алгоритмичната оценка, която е в съответствие с правото. В крайна сметка проучването заключава, че институционалното утвърждаване на хибридната роля е незаменима предпоставка за отговорно и съобразено със закона управление на ИИ в бизнеса, основан на знания.*
Ключови думи: *изкуствен интелект; управление на знанията; хибридна правна роля; управление на изкуствения интелект; алгоритмична отговорност*

Саския Дорис Праузе, докторант
Университет по библиотекознание и информационни технологии
София, България
E-mail: prause.saskia@gmail.com