journal of ethics in higher education

Navigating the AI Frontier

Legal, Ethical, and Societal Considerations for Artificial Personhood

Mondher Khanfir & Sana Karray

July 2024

Keywords

Artificial Intelligence, autonomous AI entity, AI system, corporate, artificial personhood, ethics, governance.

Abstract

The rapid digital transformation driven by Artificial Intelligence (AI) is reshaping innovation and operational efficiency across industries. As autonomous AI systems are becoming prevalent, they significantly influence traditional business models, societal norms, and legal frameworks. AI technologies are evolving beyond mere tools to become independent economic agents capable of generating assets, making decisions, commercializing products and services, and being accountable for their actions. This evolution requires a reassessment of traditional concepts of corporate and moral personhood, particularly as AI-driven businesses need to operate inside conventional legal frameworks. This paper explores the rise of entirely AI-driven entities with fully autonomous decision-making processes, advocating for the legal status of artificial personhood. It underscores the need for an ethical and regulatory framework to ensure these entities will proliferate and operate for human progress with integrity and responsibility.

Corresponding Authors: Mondher Khanfir & Sana Karray, Emails: mondher@khanfir.info, sana.karray@gmail.com. To quote this article: Khanfir, Mondher & Karray, Sana. 2024. “Navigating the AI Frontier: Legal, Ethical, and Societal Considerations for Artificial Personhood”, *Journal of Ethics in Higher Education* 4(2024): 123–142. DOI: 10.26034/fr.jehe.2024.5965

1. Introduction: The advent and proliferation of fully autonomous AI Entities

Business operations have evolved significantly from their origins in individual proprietorships, where single traders wholly owned and managed their enterprises. As commerce grew and became more complex, the demand for larger capital investments spurred the development of partnerships and joint-stock companies. This transition marked the advent of moral personhood, legally acknowledging businesses as distinct from their owners, conferring benefits like limited liability, perpetual succession, and the capacity to own property, sue, and be sued.

The establishment of moral personhood during the Industrial Revolution was crucial, enabling private businesses to flourish and manage risks at unprecedented scales. Similarly, the modern digital era has introduced autonomous AI systems as a new frontier. In her seminal 2022 work: "Gradient Legal Personhood for AI Systems", Diana Mocanu explores the potential for these entities to be granted varying degrees of personhood within legal frameworks. Mocanu proposes a gradient theory of legal personhood, which suggests that AI systems could possess partial legal capacities tailored to their specific functionalities and societal roles. This nuanced approach highlights the complex implications of recognizing AI systems as legal entities, underscoring the need for a thorough consideration of the rights, responsibilities, and ethical dimensions associated with autonomous agents. Her analysis calls for legal innovation that accommodates the unique attributes of AI, suggesting that traditional legal categories are inadequate to address the realities of advanced autonomous systems.

AI technologies are quickly advancing beyond simple tools to become independent economic agents that can generate assets, make autonomous decisions, commercialize products and services, and be held accountable. For instance, autonomous vehicles do more than just navigate traffic; they interact with regulatory systems and make real-time decisions affecting public safety and urban planning. Similarly, AI-driven financial advisors independently

analyze market data to influence economic trends and individual financial outcomes.

This evolution requires a reassessment of traditional concepts of companies and moral personhood, especially as AI-driven businesses, such as those developing autonomous elder care robots or managing large-scale supply chains, begin to perform roles traditionally filled by humans. This confusion of roles raises significant legal and ethical concerns. As these AI entities continue to grow, it is imperative that our legal frameworks adapt to ensure they can function effectively and ethically within established regulatory boundaries.

In this context, artificial personhood is proposed as a legal and ethical framework to grant autonomous AI systems specific legal rights and responsibilities typically associated with humans or corporate entities. This designation would allow AI entities to hold assets, enter contracts, and face legal claims, thereby recognizing them as independent legal subjects distinct from their creators or operators. Such a paradigm shift is crucial as AI technologies continue to transcend their roles as mere tools, transforming into entities capable of significant autonomy and responsibility.

2. How trustworthy AI is? The emerging horizon of artificial personhood

Trustworthy AI systems are defined according to the High-Level Expert Group (HLEG) established by the European Commission as

> "software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best

> action(s) to take to achieve the given goal[1]. Trustworthy AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.

Kevin D. Ashley emphasizes that the impact of AI systems goes beyond enhancing operational efficiency; it fundamentally redefines business models and decision-making processes (Ashley, 2017).

Envision a future where a Trustworthy AI system can independently establish a digital legal entity, devoid of human shareholders, and autonomously manage its operations, including delivering and invoicing for services. This represents a significant shift, transforming AI from a mere tool to an autonomous agent within the business ecosystem.

The scenario of autonomous AI entities as economic agents underscores the critical role of both technological and legal innovation in shaping the future of business and governance. It highlights the need for proactive and collaborative policymaking to anticipate the complex interplay between AI advancements and societal needs. Several enabling factors advocate for the regulation of autonomous AI entities:

i. Technological advancements: Continued improvements in AI capabilities, including machine learning, natural language processing, and robotics, enable AI systems to perform complex tasks independently, such as negotiating contracts or managing financial transactions.

ii. Integration of cryptocurrency and blockchain: Technologies like blockchain can facilitate a fully digital business environment, providing a transparent and secure method for transaction processing and record-keeping without human oversight.

[1] Humans design AI systems directly, but they may also use AI techniques to optimise their design.

iii. Development of AI ethics and standards: Establishing global standards and ethical guidelines for the development and deployment of AI systems ensures they operate within agreed-upon norms, reducing risks associated with autonomous decision-making. For example, the European Union's General Data Protection Regulation (GDPR) sets strict guidelines on data privacy and protection, which AI systems must adhere to. Similarly, the IEEE's Global Initiative on Ethics of Autonomous and Intelligent Systems provides comprehensive frameworks for ethical AI development[2]. Another example is the Partnership on AI, which brings together academic, civil society, and industry experts to develop best practices for AI technologies, promoting transparency, fairness, and accountability.

Legal considerations for fully autonomous AI entities

The development of fully autonomous AI entities lays the groundwork for a legal status of "artificial personhood." Policymakers are grappling with how regulation should be articulated before these entities proliferate outside a unified legal framework, creating trans-border business models that are difficult to track and control. This necessitates adaptations in how people, organizations, and governments interact with them, impacting trade law, corporate responsibility, and even aspects of employment law.

Moreover, this scenario raises profound ethical questions about the role of autonomous AI entities in society, the potential data distortions they might generate, and their impacts on human employment and economic structures. While the scenario is rich with opportunities for innovation and efficiency, it also demands careful consideration of its broader implications.

[2] Institute of Electrical and Electronics Engineers (IEEE), IEEE (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. IEEE. https://www.ieee.org/

The following example illustrate this trend of autonomous AI entities that could potentially claim a status of artificial personhood:

Creating an open source academic platform for online degree programs

Imagine an academic platform entirely operated by AI, delivering accredited online courses to a broad audience. This platform, devoid of human intervention, uses AI to manage all aspects of its operations, from course content creation to student assessment and administrative tasks. Here's how it functions:

i. Content creation and updates: AI algorithms continuously analyze educational trends, research publications, and industry requirements to develop and update course materials, ensuring the content remains current and relevant.

ii. Student enrollment and management: The AI system handles student enrollment, including verifying credentials and prerequisites, managing course registrations, and maintaining student records. It provides personalized learning paths based on individual progress and performance.

iii. Automated teaching and evaluation: AI-driven teaching assistants provide real-time feedback, answer student queries, and facilitate discussions. AI also assesses assignments, quizzes, and exams, ensuring unbiased and consistent evaluation.

iv. Administrative operations: The platform manages financial transactions, including fee collection and fund distribution to partner institutions. It also ensures compliance with accreditation standards and regulatory requirements, maintaining transparency and accountability.

v. Continuous improvement: The AI system monitors student engagement and outcomes, using data analytics to identify areas for improvement. It adjusts teaching methods and materials accordingly to enhance the learning experience.

Importance of aligning global jurisdictions

The potential for autonomous AI entities to operate under a formal legal status underscores the necessity of harmonizing international legal frameworks. This alignment is critical for several reasons:

i. Ensuring accountability and compliance: A unified legal approach ensures that AI entities are held accountable and that their operations comply with international standards, particularly in areas like data privacy, security, and consumer protection. The management of profits and losses would require a new framework for autonomous AI entities, defining fiduciary duties and establishing mechanisms for accountability in the absence of human management.

ii. Facilitating international cooperation: As AI entities potentially operate globally, aligned legal frameworks facilitate international cooperation in oversight, enforcement, and the sharing of best practices in AI governance.

iii. Avoiding digital paradises: Without a harmonized legal framework, there could be a rise in digital paradises, i.e jurisdictions with lax regulations that might attract AI entities seeking to escape stringent controls. Such environments could undermine global efforts to manage AI responsibly and ethically.

While establishing a unified legal framework is essential for ensuring compliance and cooperation across borders, it is equally crucial to address the ethical dimensions that such frameworks intend to govern. As we navigate the complexities of international legal alignment for AI entities, we must also consider how these laws translate into ethical practices that uphold the highest standards of integrity and accountability.

3. Ethical rules and principles for artificial personhood governance

The question of ethics in business when dealing with artificial personhood may seem incongruous. How can a machine act ethically when it has no conscience? This concern has arisen for companies like Google and OpenAI, which claim to have safeguards to avoid errors. However, incidents like the Air Canada chatbot's errors in managing customer relationships show these measures are often insufficient. The necessity for ethical governance is underscored by other incidents where AI technologies have raised significant legal questions. For instance, the misuse of facial recognition technology by companies like Clearview AI, which scraped billions of images from the internet without consent, highlights the critical need for stringent data privacy controls. Similarly, Amazon's AI recruiting tool, which exhibited bias against women, illustrates the imperative to continuously refine algorithms to minimize biases.

To optimize the societal benefits of autonomous AI entities while mitigating associated risks, it is imperative to integrate specific ethical rules and principles into the framework of artificial personhood. Programs like the IEEE's Global Initiative on Ethics of Autonomous and Intelligent Systems lay the groundwork for a robust ethical foundation, crucial for enabling artificial personhood to attain legal recognition as a "corporate entity". The principles developed by this initiative form the foundation of the comprehensive list of rules and principles detailed in the matrix below:

Rule/Principle	**Description**	**Implementation**
Non-Distortion Rule	AI systems must ensure the accuracy and integrity of data. They should not distort or manipulate data to produce misleading outcomes. Transparent algorithms should be used to validate the integrity of the data.	Ensure the accuracy and integrity of data. Validate data with transparent algorithms.

Non-Domination Rule	AI systems should not exert overpowering control or influence over individuals or societal structures. Checks and balances should be incorporated to prevent undue influence.	Incorporate checks and balances to prevent undue influence.
Non-Dependency Rule	Critical societal functions should not become solely dependent on AI technologies. Human-driven systems should be maintained as alternatives. Diversification of capabilities and redundancy in critical systems should be promoted to protect against AI failures or malfunctions.	Maintain human-driven systems as alternatives. Promote diversification and redundancy.
Non-Discrimination Rule	AI systems must treat all individuals and groups fairly, without bias or prejudice. AI entities must be designed to avoid biases that could lead to discriminatory outcomes, particularly against vulnerable or marginalized populations. Continuous monitoring and auditing are essential to detect and correct any biases that may emerge over time.	Design AI to avoid biases. Conduct continuous monitoring and auditing. Promote social equity.
Transparency Principle	AI systems must be transparent in their operations. Decision-making processes should be explainable and accessible to users, stakeholders, and regulatory bodies. Regular audits should be conducted to ensure transparency and accountability in AI operations.	Make decision-making processes explainable and accessible. Conduct regular audits.

Accountability Principle	Clear accountability mechanisms must be established. Legal and ethical responsibilities should be clearly defined for the creators, operators, and maintainers of AI systems. Mechanisms for redress and remediation must be available in cases where the AI system causes harm or violates ethical guidelines.	Establish clear accountability mechanisms. Provide mechanisms for redress and remediation.
Human Rights Protection Principle	AI systems must respect and protect human rights. They should be designed and operated in ways that do not infringe on individual freedoms or rights.	Ensure AI systems respect and protect human rights.
Privacy and Data Protection Principle	AI systems must comply with all applicable data protection laws, such as GDPR. They should ensure that user data is collected, stored, and processed securely and with consent. Measures must be taken to protect user privacy and prevent unauthorized access or misuse of data.	Comply with data protection laws. Ensure secure collection, storage, and processing of user data.
Security Principle	AI systems must be secure against cyber threats and unauthorized access. Robust security protocols should be in place to protect the integrity and functionality of AI operations. Regular security assessments and updates should be conducted to address potential vulnerabilities.	Implement robust security protocols. Conduct regular security assessments and updates.

Beneficence and Non-Maleficence Principle	AI systems should be designed and operated to benefit society and minimize harm. They should avoid causing physical, psychological, or social harm. Ethical considerations should be integrated into the design and deployment of AI systems to ensure they contribute positively to society.	Design AI to benefit society and minimize harm. Integrate ethical considerations into AI design.
Responsibility and Liability Principle	AI systems must be held liable for their actions. Insurance models and liability frameworks should be established to cover potential legal and regulatory penalties. AI entities should contribute to a regulatory fund or set up escrow accounts to manage potential liabilities.	Establish insurance models and liability frameworks. Contribute to regulatory funds or escrow accounts.
Interoperability and Cooperation Principle	AI systems should be designed to cooperate with other AI and human systems, facilitating interoperability and collaborative operations. Standards for interoperability should be established and adhered to, ensuring smooth integration and cooperation across different systems and jurisdictions.	Design AI for interoperability and cooperation. Establish and adhere to interoperability standards.
Sustainability Principle	AI systems should operate sustainably, minimizing their environmental impact. They should use energy-efficient technologies and adopt practices that support environmental conservation. Environmental impact assessments should be conducted regularly to ensure sustainable operations.	Use energy-efficient technologies. Conduct regular environmental impact assessments.

4. Applicability of ethical rules and principles to an open source academic platform

To demonstrate how these rules and principles apply to the example of an Open Source Academic Platform for Online Degree Programs, we will examine each rule and principle within the context of this scenario:

Rule/Principle	**Application to Open Source Academic Platform for Online Degree Programs**
Non-Distortion Rule	Ensure the accuracy and integrity of educational data. Use transparent algorithms to validate course content and assessment data, avoiding any manipulation or misleading outcomes.
Non-Domination Rule	Implement checks and balances to prevent AI systems from exerting undue control over students or faculty. Ensure that human oversight is in place for significant decisions related to course content and student evaluations.
Non-Dependency Rule	Maintain human-driven alternatives for critical academic functions. Ensure that human educators and administrators are involved in overseeing the platform, providing redundancy in case of AI system failures.
Non-Discrimination Rule	Design AI to treat all students fairly, avoiding biases in admissions, grading, and interactions. Implement continuous monitoring and auditing to detect and correct any biases, ensuring equitable treatment of all students, including those from marginalized groups.
Transparency Principle	Make decision-making processes and algorithms used by the platform explainable and accessible to students, faculty, and regulatory bodies. Conduct regular audits to ensure transparency and accountability.

Accountability Principle	Establish clear accountability mechanisms for AI system creators, operators, and maintainers. Provide mechanisms for students to report grievances and seek remediation if the AI system causes harm or violates ethical guidelines.
Human Rights Protection Principle	Ensure that AI systems respect and protect students' rights to privacy, freedom of expression, and access to education. Design the platform to operate without infringing on individual freedoms or rights.
Privacy and Data Protection Principle	Comply with data protection laws such as GDPR. Securely collect, store, and process student data with their consent. Implement measures to protect privacy and prevent unauthorized access or misuse of data.
Security Principle	Implement robust security protocols to protect against cyber threats and unauthorized access. Conduct regular security assessments and updates to address potential vulnerabilities.
Beneficence and Non-Maleficence Principle	Design the platform to benefit society by providing accessible, high-quality education. Avoid causing physical, psychological, or social harm to students and staff. Integrate ethical considerations into the design and deployment of AI systems.
Responsibility and Liability Principle	Hold AI systems liable for their actions. Establish insurance models and liability frameworks to cover potential legal and regulatory penalties. Contribute to a regulatory fund or set up escrow accounts to manage potential liabilities.
Interoperability and Cooperation Principle	Design the platform to cooperate with other AI and human systems, facilitating interoperability and collaborative operations. Adhere to established standards for smooth integration across different systems and jurisdictions.

Sustainability Principle	Operate the platform sustainably, minimizing environmental impact. Use energy-efficient technologies and adopt practices that support environmental conservation. Conduct regular environmental impact assessments to ensure sustainable operations.

By diligently applying these rules and principles, the Open Source Academic Platform for Online Degree Programs can operate responsibly and ethically, ensuring its contributions are beneficial to society while minimizing risks and negative impacts. However, despite these safeguards, potential risks such as data breaches, algorithmic biases, and the misuse of personal information could pose significant challenges, necessitating ongoing vigilance and adaptive management strategies to protect stakeholders and maintain trust.

5. Coercive and reparative measures in case of offense or misstep

When entities with artificial personhood breach legal or ethical standards, robust coercive measures must be established to rectify any missteps and prevent future violations. These measures should be fundamentally corrective and reparative rather than purely punitive, given that traditional sanctions might not have the same impact on artificial intelligence as they do on human actors. Ensuring public trust and ethical compliance should be the primary goals.

For example, if an AI-operated healthcare provider incorrectly diagnoses patients due to an error in its learning algorithm, the response should not only involve rectifying the error but also ensuring that it does not recur. This might include mandatory audits of the AI system's decision-making processes, a temporary suspension of its diagnostic functions until the issue is resolved, and transparent communication with affected patients and the public to restore trust. Similarly, if an AI financial advisor makes unauthorized trades that benefit some clients at the expense of others, the corrective actions could involve compensating those harmed, revising the AI's operational parameters,

and implementing stricter oversight mechanisms to monitor its trading behaviors.

Furthermore, in cases where AI-driven content moderation systems on social media platforms fail to detect and prevent the spread of harmful misinformation, not only should the algorithms be adjusted, but measures should be taken to educate the AI on recognizing such content more effectively. Public reporting on the steps taken to correct these oversights and the introduction of more rigorous testing phases before updates are deployed can help maintain user trust and compliance with ethical standards.

These examples highlight the need for AI systems with personhood to operate under frameworks that prioritize adaptability, accountability, and transparency, ensuring that any breach of ethics or law is met with responses tailored to correct and improve the system rather than merely punish.

To address these challenges effectively, it is essential to implement a dual approach of coercive and reparative measures, ensuring not only that missteps are corrected but also that future violations are systematically prevented.

Coercive measures can include:

I. Operational restrictions: Imposing limitations on the AI entity's operational capabilities to prevent further harm and prompt immediate corrective action. This might involve restricting certain functions until compliance is restored.

II. Revocation of licenses: For serious violations, the AI entity's operational licenses can be revoked, serving as a significant deterrent and emphasizing the importance of adhering to legal and ethical standards.

III. Implementation of an ethics review board: Establishing an ethics review board within the organization to oversee compliance. This board would proactively maintain ethical standards, review new AI systems before launch, and ensure continuous adherence to established guidelines. The board should have the authority to halt or modify AI operations if ethical breaches are identified.

Reparative measures should complement coercive actions to address and rectify any harm caused by the AI entity. These can include:

i. Mandated remediations: Requiring AI entities to take specific actions to remedy any harm caused. This could involve correcting biased algorithms, improving data security measures, or enhancing transparency in their operations.

ii. Public apologies and transparency reports: Issuing public apologies to restore public trust. Additionally, mandating transparency reports that detail the violation, the steps taken to address it, and measures implemented to prevent recurrence. These reports should be accessible to the public and regulatory bodies to ensure accountability.

By integrating coercive and reparative measures, the framework ensures that AI entities remain accountable and operate within the bounds of ethical and legal standards. This approach addresses immediate issues while fostering a culture of continuous improvement and ethical integrity within the realm of artificial personhood.

Collaboration among policymakers, industry leaders, and the global community is crucial in shaping a future where these autonomous AI agents are legalized through artificial personhood, endorsing norms of corporate societal responsibility and compliance. This important shift in the corporate landscape will undoubtedly raise many challenges, such as:

i. Corporate structure revisions: Artificial personhood companies might be required to register as separate legal entities, similar to traditional corporations, capable of independently owning assets, incurring debts, and being liable for fines.

ii. Asset allocation: During the formation of such companies, specific provisions could be made to allocate assets for covering potential legal liabilities.

iii. Insurance models: Implementing liability insurance models to cover legal and regulatory penalties could adapt traditional business practices to the needs of autonomous entities.

iv. Regulatory fund: Establishing a fund specifically designed to manage fines imposed on AI-driven entities could be considered, with companies contributing as part of their licensing requirements.

v. Escrow or trust account: Setting up a trust or escrow account, funded from portions of their revenues or initial capital, could be mandated to cover legal and regulatory fines.

vi. Government oversight: In scenarios lacking human oversight, a state-controlled body could be appointed to oversee the financial and legal responsibilities of artificial personhood companies, ensuring compliance with established legal standards.

These proposals are designed to ensure that artificial personhood remains accountable and compliant even in the absence of direct human control. As we progress into an era of increasing AI autonomy, these innovative legal adaptations are crucial. Each approach has its own set of merits and challenges and would require careful design to balance operational efficiency with societal and legal safeguards. Ultimately, legislative changes and innovative legal structures will be vital as we redefine the role of a company in the age of autonomous AI.

6. Conclusion

Artificial personhood stands at the frontier of business and technology, embodying immense potential as well as significant risks. The previous sections showed how the rapid evolution and integration of autonomous AI agents into business operations necessitate robust legal, ethical, and regulatory frameworks that keep pace with technological advancements. This situation requires careful examination and potential reformation of corporate and legal structures to accommodate the unique characteristics of autonomous AI agents.

The journey towards the legalization of autonomous entities led by AI opens up vast possibilities for human progress, notably enhancing productivity and inclusiveness across various sectors. These advancements, however, bring to the forefront critical issues that extend beyond the ethical considerations typically associated with AI deployment. Among these is the imperative question of how the wealth generated by these entities is distributed. This concern transcends the realm of ethics, touching upon the principles of intellectual property and taxation—areas that require robust frameworks to ensure that benefits are shared equitably. As we navigate these complexities, it becomes clear that these are not merely technical or regulatory issues but are deeply intertwined with the socio-economic fabric of our societies. Exploring these domains will be essential as we continue to integrate AI more deeply into our daily lives and global economy, ensuring that progress is not only advanced but also just and inclusive for all.

7. Bibliography

Ashley, Kevin D. 2017. *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*. Cambridge: Cambridge University Press.

Crawford, Kate, Roel Dobbe, Theodora Dryer et al. 2019. AI Now 2019 Report. New York: AI Now Institute.

European Commission. High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

European Commission. Artificial Intelligence Act. 2021.

Holdsworth, William S. 1922. *A History of English Law*. 3 Vol. Boston Little, Brown and Cie, third Ed.

Institute of Electrical and Electronics Engineers (IEEE), IEEE (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. IEEE.

https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v2.pdf

Lamoreaux, Naomi R. and William J. Novak. 2017. *Corporations and American Democracy*. Cambridge: Harvard University Press, 528pp.

Micklethwait, John, & Wooldridge, Adrian. 2003. *The Company: A Short History of a Revolutionary Idea.* Modern Library. Sect. 2: "Legal Challenges Posed by AI".

Mocanu, Diana Mădălina. "Gradient Legal Personhood for AI Systems—Painting Continental Legal Shapes Made to Fit Analytical Molds". *Frontiers in Robotics and AI*, Vol. 8, 2022: 1-11. https://doi.org/10.3389/frobt.2021.788179

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publ. 259pp.

Păvăloaia V-D, Necula S-C. "Artificial Intelligence as a Disruptive Technology A Systematic Literature Review". *Electronics*, 12, no. 5, 2023: 1102. https://doi.org/10.3390/electronics12051102

Peres, R.S., Jia, X., Lee, J., Sun, K., Colombo, A.W., & Barata, J. "Industrial Artificial Intelligence in Industry 4.0 - Systematic Review, Challenges and Outlook", in *IEEE Access*, vol. 8 (2020): 220121-220139, https://doi.org/10.1109/ACCESS.2020.3042874

Russell, Stuart, & Norvig, Paul. 2010. *Artificial Intelligence. A Modern Approach*., 3rd Ed., Oxford: Prentice Hall.

8. Short biography

Mondher Khanfir leads the influential For a Shared Prosperity in Africa Think Tank. His commitment to leveraging innovation for social and economic progress has catalysed his engagement across Africa and the MENA region. Mondher's focus lies in guiding governments to cultivate

innovation ecosystems and oversee infrastructure projects, enhancing their integration into global value chains.

His prolific contributions include authoring numerous reports and spearheading initiatives to implement Research & Innovation programs. He has conducted pivotal research studies on private sector competitiveness and provided insightful analysis on capital market development in emerging economies.

Email: mondher@khanfir.info

Sana Karray has a PhD in management. She graduated in accounting then pursued a Master's degree in management and performed her thesis on social capital in family businesses (Sorbonne University, Paris: 2014). Sana has been teaching in accounting, auditing, business strategy, innovation management, and entrepreneurship at public and private universities. She is actively participating in associations that support entrepreneurs in initiating their ventures, emphasizing business model assessment and implementation. Sana has as current research interest the transformative effects of artificial intelligence on the corporate environment.

Email: sana.karray@gmail.com