What managers of SMEs in the CEE region should know about challenges of artificial intelligence's adoption? – an introductive discussion

Co menedżerowie MŚP w regionie Europy Środkowo-Wschodniej powinni wiedzieć o wyzwaniach związanych z wprowadzeniem sztucznej inteligencji? – dyskusja wprowadzająca

Cristian-Mihai Vidu

National University for Political Sciences and Public Administration (SNSPA), Bucharest, Romania
cristian.vidu@facultateademanagement.ro; ORCID: 0000-0001-9242-6313

Florina Pinzaru

National University for Political Sciences and Public Administration (SNSPA), Bucharest, Romania
florina.pinzaru@facultateademanagement.ro; ORCID: 0000-0002-8371-5284

Andreea Mitan

National University for Political Sciences and Public Administration (SNSPA), Bucharest, Romania
ORCID: 0000-0002-7988-6638

Abstrakt. The next step of the digital transformation is to adopt artificial intelligence (AI), even if the technology itself is still evolving. Nevertheless, discussions on AI pros and cons are vivid: managers are in the frontline of the decision-making on the best ways for such transitions. If corporations are already familiar with AI, at least partially for some processes, small and medium enterprises (SMEs) face a double pressure: their inequal degree of digital maturity, as well as the everyday constraints on how to increase competitiveness. CEE SMEs, in particular, find themselves in a complex framework, and the adoption of AI, even if challenging, could be one of the solutions to advance in terms of efficiency. Nevertheless, risks in such an approach must be carefully considered. Based on a semi-structured literature review, this opinion paper discusses the main risks that managers of SMEs in the CEE region should understand regarding AI and the consequent challenges of adopting it in business. Final considerations and future research discussions conclude the paper.
Słowa kluczowe: European SMEs' digital transformation; artificial intelligence adoption; risk management

Abstract. Kolejnym krokiem cyfrowej transformacji jest przyjęcie sztucznej inteligencji (AI), nawet jeśli sama technologia wciąż ewoluuje. Niemniej jednak dyskusje na temat zalet i wad AI są żywe: menedżerowie znajdują się na pierwszej linii podejmowania decyzji dotyczących najlepszych sposobów wprowadzenia takich zmian. Jeśli korporacje są już zaznajomione ze sztuczną inteligencją, przynajmniej częściowo w przypadku niektórych procesów, małe i średnie przedsiębiorstwa (MŚP) stoją przed podwójną presją: nierównym stopniem dojrzałości cyfrowej, a także codziennymi ograniczeniami w zwiększaniu konkurencyjności. W szczególności MŚP z Europy Środkowo-Wschodniej znajdują się w skomplikowanych ramach, a przyjęcie sztucznej inteligencji, nawet jeśli jest trudne, może być jednym z rozwiązań umożliwiających postęp pod względem wydajności. Mimo wszystko ryzyko w takim podejściu musi być dokładnie rozważone. Opierając się na częściowo ustrukturyzowanym przeglądzie literatury przedmiotu, w niniejszym artykule omówiono główne zagrożenia, które menedżerowie MŚP w regionie Europy Środkowo-Wschodniej powinni zrozumieć w odniesieniu do sztucznej inteligencji, i wynikające z niej wyzwania związane z jej przyjęciem w biznesie. Końcowe rozważania i przyszłe dyskusje badawcze zamykają prace.
Keywords: transformacja cyfrowa europejskich MŚP; przyjęcie sztucznej inteligencji; zarządzanie ryzykiem

Introduction

Digital transformation is a reality and a recognized necessity in today's companies. Deloitte (2019) defines it as the use of technology to evolve the business models and several recent studies (Accenture, 2021). Various authors (Calp, 2020; Kitsios, Kamariotou, 2021) have recognized that one of the essential technologies driving digital transformation is represented by artificial intelligence. McKinsey Global Institute goes as far as to call it "the next digital frontier" (Bughin, Hazan, Ramaswamy, Chui, Allas, Dahlström, Henke, Trench, 2017), which serves to emphasize the increasing importance of AI in today's business environment.

In the context of transforming the enterprise into an agile, digitally enabled, future-proof entity, artificial intelligence is one tool that no business leader cannot neglect. However, in general, digital transformation is admittedly hard to get right, and, consequently, many projects fail (Davenport, Redman, 2020). Also, as the technology matures and adoption increases, managing the risks associated with its usage becomes more important. If, in the early adoption days, the risks were set aside to allow for fast progress in the face of disruptive technologies, managing risk becomes critical as time progresses. One study by KPMG (2018) revealed that only 34 percent of the IT managers that adopted artificial intelligence technologies had assessed their risks. Accenture complements and accentuates this view with a later study which shows that only 11% of risk managers consider themselves as knowing to assess the risks that may come with AI (Accenture, 2019). This leads to a significant reduction in the declared rate of adoption of AI technologies in organizations due to the emerging risks (Ammanath, Jarvis, Hupfer, 2020).

The present paper proposes investigating the business risks associated with AI adoption as presented in the current literature through the prism of their impact in the case of SMEs in the CEE region. The paper is structured in the following main parts: an introduction regarding CEE SMEs to better pinpoint their business framework and digital maturity; a presentation of the significant aspects to be

considered regarding artificial intelligence and digital transformation, covering the general types of risks associated with AI and digitalization; a detailed analysis of the business risks associated with AI adoption in general and in the case of European SMEs in particular; a discussions section.

CEE SMEs on the path to business competitiveness and digital transformation

Over 90% of the extant companies operating today in the world are SMEs, mobilizing approximately 50% of the global workforce (World Bank, 2022). These companies' contribution to the national income (GDP) is significant: up to 40% of the total GDP is linked to formal SMEs, and other significant but variable percentages are owed to informal SMEs. The importance of SMEs as economic actors and employers is estimated to become even higher in the years to come, as 600 million jobs are expected to be needed by 2030 to absorb the growing global workforce. According to the World Bank (2022), SMEs will play a vital role in the economies of emergent countries, generating 7 out of 10 jobs. The competitiveness and business performance of those SMEs both on their domestic and on the international markets, and their capacity to learn, to adopt new technologies, and to adapt to new standards, are vital for the welfare of the stakeholders, as well as for the economic and political stability in the regions where they operate (Vătămănescu, Andrei, Nicolescu, Pinzaru, Zbuchea, 2017; Vătămănescu, Gorgos, Ghigiu, Pătruţ, 2019).

Nonetheless, the European Union acknowledges the importance of SMEs in supporting its mission and conferring predictability to its economic development prospects. In this sense, an array of measures has been adopted since the launch of the Small Business Act (2008) in order to support entrepreneurs and SMEs, leading to a single consolidated market. Progress has been made in key areas of the community space. However, much is still to be accomplished, as only around 25% of the SMEs from the member states benefit from the opportunities offered by the single market in the area of exports (European Commission, 2020).

In the CEE region, SMEs vary from one country to another. In 2018, Romania reportedly had 29 SMEs per 1000 inhabitants, while the Czech Republic had 115 SMEs per 1000 inhabitants, the EU-28 median being 58 SMEs/1000 inhabitants (Hope, 2019). However, the Romanian authorities have taken several steps since 2008 towards supporting the local SMEs and entrepreneurs, improving the state aid schemes, granting access to financing instruments, improving the administration, and supporting business internationalization initiatives (DIW ECON, 2018). Studies have shown potential in studying the CEE region, as business development has been impacted in this area by many context-driven particularities (Jaklič, Obloj, Svetličič, Kronegger, 2020). These countries have undergone "a great transformation"

(Kornai, 2008) since the fall of the European communist regimes during the 1990s. Contemporary SMEs from the CEE region emerged and grew in conditions that are widely different from those other European counterparts had to deal with (Whitley, Czaban, 1998), displaying unique features. As Meyer and Peng (2005) acknowledge, the ground that CEE countries offer for future analysis is fertile, as context-sensitive researchers can find insight, by studying it, regarding how the shifting identities, evolving political perspectives, transitioning organizations, economic and social transformations impact the realms of business and economy. Stemming from the historical conditions, intertwined with the political and economic particularities that former communist countries in the CEE region have, the richness of the context led various researchers to underline the importance of conducting in-depth studies concerning the business environment, SMEs and business internationalization processes in the area (Soulsby, Clark, 2007; Meyer, Peng, 2016). This sort of endeavor favors the expansion of knowledge regarding the behavior of the SMEs on domestic and foreign markets, bringing to the fore the opportunity of theoretical gains, adding to the extant literature which is mainly focused on Western companies and conditions of business development (Jaklič, Rašković, Schuch, 2018). While the literature has started to cover some of the countries in the CEE, reporting on Poland, Hungary, Estonia, the Czech Republic, and Slovenia (Ipsmiller, Dikova, 2021), more is yet to be learned by studying the other countries in the region and by conducting comparative analyses that would offer a more detailed picture of the regional dynamics and lore (Jormanainen, Koveshnikov, 2012).

The overall environment of CEE SMEs is complex, revealing a strong pressure for such enterprises to be durably competitive, and their digital transformation is one of the solutions to advance on the path of competitiveness. The adoption of AI, in particular, could substantially affect SMEs' business environment, from influences driven by changes of regulations and competition to "improving SMEs' access to finance, easing skills management and job matching, or reducing the costs of experimentation and innovation" (OECD, 2021). Despite potential benefits, the adoption of AI could lead to numerous challenges, as there is already evidence of SME gaps in implementing AI solutions (OECD, 2021). AI can affect SMEs in two ways: altering their business environment or enabling them to change business models and thus become more competitive. SMEs are at the core of the CEE economy, but the COVID-19 pandemic has revealed their fragility and the need for effective digitalization and upskilling (PwC, 2021).

Nevertheless, the digital readiness of SMEs is subject to debate. For instance, in the case of Latvian SMEs, a major factor enhancing the adoption of digitalization, in general, is public financial support (Rupeika-Apoga, Bule, Petrovska, 2022). These findings are coherent with the overall situations of CEE economies, still struggling to catch up with the advances of digitalization at the level of businesses (Trașcă, Stefan,

Sahlian, van Hoinaru, Serban-Oprescu, 2019). However, digitalization seems to be a key factor for SMEs to become more competitive in Hungary (Bughin, Janoskuti, Havas, 2016). SMEs of the CEE region face the same challenges in terms of business digital maturity as the overall economies, with the lowest results in the case of Romania, Bulgaria, Latvia, and Hungary: "among the most important left-skewed asymmetric distributions are to be found for analysis of big data from smart devices or sensors", "analysis of big data from the geolocation of portable devices", "use of smart meters, smart lamps, smart thermostats to optimize energy consumption in the enterprise's premises", and "enterprises that provide training to develop/upgrade ICT skills of their personnel", varying depending on enterprise size and sector of activity (Tutak, Brodny, 2022). The situation of software SMEs from the CEE region should be considered apart, and it is not treated in this paper.

Understanding AI: the next step of the digital transformation

While there is no agreed consensus on what exactly is artificial intelligence or how it can be universally defined (Fogel, 2006) and there are also opinions that AI is that technology that "is never really here" (Davenport, Bean, 2018), we will adopt a working definition of AI-based on Russel et al. (2020) who define it as that which "enables the machine to exhibit human intelligence, including the ability to perceive, reason, learn, and interact". This definition is quite broad, and it allows for multiple interpretations. The most general interpretation, which looks at an artificial intelligence capable of functioning over a broader context and in many distinct domains, is represented by the so-called Artificial General Intelligence (AGI) (Yudkowsky, 2008). This type of artificial intelligence has the highest potential for disruption, but currently, AGI is still at the level of research (Dambrot, 2020), not at commercial availability. AGI carries its own set of risks, and some consider that it carries a set of profound existential risks to the future of humanity (Bostrom, 2017; Yudkowsky, 2008), though there is also the alternative current that it will enable the next step of evolution for the human race (Kurzweil, 2013).

In contrast to the generality and vast capabilities of AGI, Artificial Narrow Intelligence (ANI) has applications over specific functionalities with algorithms capable of performing specific tasks. The advantage of this approach is that after designing a narrow AI algorithm capable of performing specific tasks at an average human level, due to raw computational power, it takes very little time to improve it to perform the same tasks at the above human level. The general perception is that all technologies currently available under the broad term of artificial intelligence fall under this ANI category (Al-Shabandar, Lightbody, Browne, Liu, Wang, Zheng, 2019; Kaplan, Haenlein, 2019).

The distinction between the two types of artificial intelligence is essential for the focus of this paper. Our focus will be on managers' immediate risks when adopting commercially available AI technologies, such as ANI. Some examples of directly applicable technologies which would fall under this term are machine learning (Canhoto, Clear, 2020), deep learning (Lu, 2019), natural language processing (Kietzmann, Pitt, 2020), computer vision (Brynjolfsson, McAfee, 2014), speech recognition (Jarrahi, 2018) etc.

Challenges in adopting AI: what should managers of SMEs in the CEE region know?

The academic literature on the business risks of artificial intelligence is only just developing. However, authors already consider various risks that managers should be aware of when investing in AI, such as regulations, privacy issues, legal liability, biases, explainability, costs, and cybersecurity. We will briefly present them below, pointing out the necessity to allocate more financial and human resources for understanding them: if corporations have legal, IT, and compliance departments dedicated to such activities, they are almost unknown to SMEs in general and to those from the CEE region in particular, where the degree of digital maturity is very diverse, but in general lower than in the rest of the EU.

The evolving constraints of the regulatory framework

If before 2020, artificial intelligence for commercial use was not regulated in the EU, in 2020 European Commission revealed a broad legislative proposal for public consultation and feedback (Stuurman, Lachaud, 2022). By 2021 the full regulatory, legislative proposal had already been drafted and submitted (European Commission, 2021), which applies a risk-based approach to the development and adoption of AI-driven products, services, and systems with increasing oversight and regulation risk increase (Kop, 2021). This is considered the first-ever horizontal regulation of artificial intelligence at the European level (Madiega, 2021). While regulatory frameworks can benefit-risk reduction by cutting the exposure companies face when adopting AI, it can also pose a challenge due to the lack of consensus in worldwide regulation efforts and the complications faced when trying to follow divergent views. This is especially true in a field such as artificial intelligence, where regulation is only emerging and where even the definition of AI is in a state of flux. Compliance, in this case, becomes a significant concern, but it is a concern that some enterprises are accustomed to, and lessons learned from banks and insurance companies can

be applied. Some researchers even suggest using AI to help with the compliance function (Königstorfer, Thalmann, 2020). However, some of the contexts discussed, such as using AI to detect non-compliance by analyzing conversations, introduce a different type of risk, the privacy risk. Managers of SMEs need to carefully watch for updates of regulations at EU and national levels to comply with specific issues regarding the use of AI.

The potential risk of privacy issues

Privacy is directly related to personal data and represents, according to GDPR, the specific type of information which can be used to identify, either directly or indirectly, or is related to an individual (Koch, 2019). At first glance, privacy, due in part to the effect of GDPR but also other existing regulations already enacted in most countries, is a distinct category of risk, not directly tied to artificial intelligence. Even supposedly public or anonymized data could become private or sensitive. This breach of privacy, in turn, can lead to potential legal liability. GDPR is mandatory in the EU, and managers are aware of it; therefore, complying with it in the case of AI's adoption should not be a major challenge for SMEs already accustomed to it for other digital instruments.

Legal liability

Legal liability is becoming a complex topic as artificial intelligence expands beyond the simple rule-based expert systems of the past and increases its reach into organizations. The problem set forth here is who is, in the end, responsible and, in this context, who can be held accountable for decisions made or assisted by artificial intelligence as it gains more autonomy. Straub (2021) states that the liability of treating AI as a product could extend to both the designers and operators of the product, and this has the potential to further add to the complexity due to the different jurisdictions that they can be in. While some view that product liability would be difficult to apply (Čerka, Grigienė, Sirbikytė, 2015), additional considerations should be reviewed when looking at AI as not only a product but a service. Cobbe et Singh (2021) argue that in this context, the providers themselves may be liable for illegal activities carried out by their customers using the services they provide. This context brings forward the additional risk of criminal liability, and here is where specific SMEs should pay attention to, by looking carefully at legal evolutions on the topic at the EU and national levels.

The concern regarding biases

Bias is a concern because the way that artificial intelligence and machine learning algorithms have been working, at least in a significant part, is by identifying patterns in data after being subjected to large datasets and learning from those datasets. This approach works quite well for the cases where the datasets are representative of the general population from which they are drawn, as the large volume of data corrects any minor inconsistencies. However, this approach starts to break down when dealing with unrepresentative data, as this will potentially bias the algorithms' decisions, potentially opening the way for discrimination. Bias is tough to estimate and even more challenging to eliminate as it can come from multiple sources.

When looking at decisions made in this context, their impact depends on the role of AI: that of a recommender system, which delegates the final decision to the human receiving the recommendation, or that of a top decision-maker where the decisions are incorporated into the managerial processes and are more difficult for people to refute them (Lee, 2018). Wagner (2019) suggests that, even when the algorithm is still working as a recommender system, and the final decision is left to a human, the fundamental role of the human is only to "rubber-stamp" the decision made by the algorithm and to reduce the legal liability risks discussed earlier. SME managers need in such an approach pay bigger attention than usual to such matters.

Explainability

One possible way that can allow for the mitigation of bias is by using explainable AI (XAI), which refers to the ability to describe how a model reached a particular decision on one hand and to the ability to explain the model itself, the inner workings of the model, on the other (Belle, Papantonis, 2021). The argument for explainability is not a purely technical one, as research points to the fact that advice from AI systems would be more acceptable to humans if the advice could be explained to them (de Bruijn, Warnier, Janssen, 2021), posing unexpected challenges to managers. A major difficulty in this sense is related to the fact that in the CEE, the business population is not very familiar with data analytics (OECD, 2021); thus, we can assume that the mindset in SMEs as well is still not oriented towards processing such variables for deciding what AI solutions to be adopted.

Separate from the increase in trust, the ability to explain how a decision was made is also essential from a regulatory perspective. Any organization that processes the personal data of EU citizens is subject to GDPR and, under GDPR provisions, Selbst et Powles (2017) argue that there is a requirement for the users of AI models to provide "meaningful information about the logic involved". This explanation, which refers to the reasons for reaching a specific decision, presents a significant problem

for the so-called black-box algorithms such as deep neural networks, which do not have an internal representation that can be understood or verifiable, even by experts (de Bruijn, Warnier, Janssen, 2021). Thus, managers of SMEs should be aware of the possible vulnerabilities of the adopted AI solutions from this perspective.

Costs

Adopting AI in business is definitely a choice to diminish costs and increase efficiency, but paradoxically, it leads to new costs: "building and maintaining an AI system remain a costly investment (…) and an effective implementation of AI solutions requires developing and adopting complementary technologies, whereas SMEs lag behind large firms in all technological areas" (OECD, 2021). Moreover, adoption of AI is costly not only because of technical reasons but also because it requires adaptations of business processes and skills and adaptions of technology to those – and it costs. Costs of the adoption of AI are even more evident when the expected benefits, such as productivity gains, are not immediate. Operating a business in an AI-reframed context requires more skills (OECD, 2021; Loureiro, Guerreiro, Tussyadiah, 2021): training for managers to rethink business processes and reconfigure organizational tasks and structures; experienced workers in algorithmically guiding their daily activities; workers able to correlate data as even if AI systems can find patterns and correlation in existing data, they are not yet able to explain causality and still do not adapt their forecasts quickly in case of such major changes (Heaven, 2020, cited in OECD, 2021). Simply said, working with AI requires even more skilled and educated intellectual capital, which is more expensive and thus, adds new costs for SMEs.

Cybersecurity

Everything digital is subject to cybersecurity risks, and the threat of AI's adoption is important. It is indeed enthusiasm about the potential of AI for improving cybersecurity (Morel, 2011), but there are also concerns regarding the duo AI-cybersecurity in practice (Taddeo, McCutcheon, Floridi, 2019). In the case of SMEs, such threats are even more significant, as SMEs, in general, tend to ignore the possible perils of lack of appropriate cybersecurity and consequences for their businesses (Bada, Nurse, 2019). Considering the lack of sufficient financial and human resources to treat the challenges of AI cybersecurity in the case of individual SMEs, researchers have already suggested the possibility to standardize regulations, standards, and instruments (Ozkan, Spruit, 2021). SMEs with IT departments already have various experiences with cybersecurity. However, in the case of the ones lacking such structures, managers' technical education and risk management strategies are key factors for investing in such frameworks and instruments.

Instead of conclusions: discussions and future research considerations

SMEs of the CEE region are very diverse. However, in general, they are not, in their vast majority, among the digital champions, as one can deduce from the evolution of DESI (the Digital Economy and Society Index) at the European level – mainly because of insufficient financial resources, insufficient financial public support, and, more importantly, because of a managerial mindset that does not favor the wide adoption of digital instruments, and the subsequent restructuring of business processes and structures. However, considering the specificities of doing business at present, as well as the factors framing the overall CEE environment, SMEs from these countries are under real pressure to invest wisely for increasing their competitiveness: one of the solutions is accelerating the digital transformation, and, as a next step, the adoption of AI systems. Beyond chatbots, RPA software, and learning machines, AI's adoption raises new challenges for enterprises that are not yet digitally mature and lack financial resources and sufficient intellectual capital, such as many SMEs. However, the adoption of AI is not optional for SMEs in the quest for competitiveness.

This opinion paper, structured on a literature review, is a manifesto for managers of SMEs from the CEE region to consider fundamental challenges of AI, such as the progress of regulations, legal liabilities, cybersecurity concerns, consequential biases, costs, explainability, and privacy issues. AI represents more than just a new digital instrument: it is already here to reshape business, with direct and indirect consequences on processes, operations, and management practices. Every manager deciding on adopting AI systems should be aware of potential benefits, costs, and conceptual challenges as the ones the authors mentioned in this paper. The debate on the topic is only emerging, and much more research should be expected in the future. Some directions that could be developed are the investigation of perceptions of managers from SMEs in the CEE region on the benefits and risks of the adoption of AI and the degree of readiness to transform their businesses in such a perspective.

REFERENCES

[1] ACCENTURE, 2019. *2019 Global Risk Management Study*, https://www.accenture.com/us-en/insights/financial-services/global-risk-study (17.01.2022).

[2] ACCENTURE, 2021. Scaling Digital Transformation with Future Systems. Accenture. Retrieved from HTTP DIW ECON, *SMEs Performance Review 2017/2018*. www.diw-econ.com (18.05.2018).

[3] AL-SHABANDAR, R., LIGHTBODY, G., BROWNE, F., LIU, J., WANG, H., ZHENG, H., 2019. The Application of Artificial Intelligence in Financial Compliance Management, *Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing, AIAM 2019*. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3358331.3358339 (10.01.2022).

[4] AMMANATH, B., JARVIS, D., HUPFER, S., 2020. *Thriving in the era of pervasive AI Deloitte.*

[5] ARAUJO, T., HELBERGER, N., KRUIKEMEIER, S., DE VREESE, C.H., 2020. In AI, we trust? Perceptions about automated decision-making by artificial intelligence, *AI and Society*, No. 35(3).

[6] BADA, M., NURSE, J.R., 2019. Developing cybersecurity education and awareness programmes for small-and-medium-sized enterprises (SMEs), *Information & Computer Security*, No. 27(3).

[7] BELLE, V., PAPANTONIS, I., 2021. Principles and Practice of Explainable Machine Learning, *Frontiers in Big Data*, No. 4.

[8] BOSTROM, N., 2017. *Superintelligence*, Dunod.

[9] BRYNJOLFSSON, E., MCAFEE, A., 2014. *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*, WW Norton & Company.

[10] BUGHIN, J., HAZAN, E., RAMASWAMY, S., CHUI, M., ALLAS, T., DAHLSTRÖM, P., HENKE, N., TRENCH, M., 2017. *Artificial intelligence: The next digital frontier?*, McKinsey Global Institute.

[11] BUGHIN, J., JANOSKUTI, L., HAVAS, A., 2016. *The next gold medal: How Hungary can win the productivity race in the digital age*, McKinsey Global Institute.

[12] CALP, H.M., 2020. *The Role of Artificial Intelligence Within the Scope of Digital Transformation in Enterprises*, [in:] Gülay, E., Alptekin, E., Birgit, O. (eds.), *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business*. Hershey, PA, USA: IGI Global.

[13] CANHOTO, A.I., CLEAR, F., 2020. Artificial intelligence and machine learning as business tools: A framework for diagnosing value destruction potential, *Business horizons, artificial intelligence and machine learning*, No. 63(2).

[14] ČERKA, P., GRIGIENĖ, J., SIRBIKYTĖ, G., 2015. Liability for damages caused by artificial intelligence, *Computer Law & Security Review*, No. 31(3).

[15] COBBE, J., SINGH, J., 2021. Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges, *Computer Law & Security Review*, No. 42.

[16] DAMBROT, S.M., 2020. Theoretical and hypothetical pathways to real-time neuromorphic AGI/post-AGI ecosystems, *Procedia Computer Science, Postproceedings of the 10th Annual International Conference on Biologically Inspired Cognitive Architectures. BICA 2019*, No. 169.

[17] DAVENPORT, T.H., BEAN, R., 2018. Big companies are embracing analytics, but most still don't have a data-driven culture, *Harvard Business Review*, No. 6.

[18] DAVENPORT, T.H., REDMAN, T.C., 2020. Digital Transformation Comes Down to Talent in 4 Key Areas, *Harvard Business Review*, May.

[19] DAWID, H., MUEHLHEUSSER, G., 2022. Smart products: Liability, investments in product safety, and the timing of market introduction, *Journal of Economic Dynamics and Control*, No. 134.

[20] DE BRUIJN, H., WARNIER, M., JANSSEN, M., 2021. The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making, *Government Information Quarterly*, 101666.

[21] Deloitte Digital, 2019. *Digital transformation: A PRIMER*, https://www.wired.com/brand-lab/2019/10/deloitte-digital-transformation-a-primer/ (22.05.2021).

[22] DIW ECON, 2018. *SMEs Performance Review 2017/2018*, https://ec.europa.eu/docsroom/documents/32601/attachments/3/translations/en/renditions/native (02.03.2020).

[23] European Commission, 2008. *Think Small First. A Small Business Act for Europe* COM (2008) 394 final.

[24] European Commission, 2003. *COMMISSION RECOMMENDATION of May 6 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/E.C.)*.

[25] European Commission, 2015. *European User guide to the SME Definition*. Ref. Ares (2016) 956541 – 24/02/2016.

[26] European Commission, 2020. *Entrepreneurship and small and medium-sized enterprises (SMEs)*.

[27] European Commission, 2021. *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts.*

[28] Fogel, D.B., 2006. *Evolutionary computation: Toward a new philosophy of machine intelligence. Vol. 1*, John Wiley & Sons.

[29] Frey, C.B., Osborne, M.A., 2017. The future of employment: How susceptible are jobs to computerisation?, *Technological forecasting and social change*, No. 114.

[30] Heaven, W., 2020. *Our weird behavior during the pandemic is messing with AI models*, https://www.technologyreview.com/2020/05/11/1001563/covid-pandemic-broken-ai-machine-learning-amazon-retail-fraud-humans-in-the-loop/?truid=538165e6a853542703d07b8605ff2f0f&utm_source=the_algorithm&utm_medium=email&utm_campaign=the_algorithm.unpaid.engage (15.02.2021).

[31] Hope, K. (ed.), 2019. *ANNUAL REPORT ON EUROPEAN SMEs 2018/2019*. Research & Development and Innovation by SMEs, https://op.europa.eu/en/publication-detail/-/publication/b6a34664-335d-11ea-ba6e-01aa75ed71a1/language-en/format-PDF/source-search (10.05.2020).

[32] Ipsmiller, E., Dikova, D., 2021. Internationalization from central and Eastern Europe: a Systematic Literature Review,*Journal of International Management*, No. 27(4).

[33] Jaklič, A., Obloj, K., Svetličič, M., Kronegger, L., 2020. Evolution of Central and Eastern Europe related international business research, *Journal of Business Research*, No. 108(C).

[34] Jaklič, A., Rašković, M., Schuch, A., 2018. Examining the Contextual Richness of Central and Eastern Europe, *AIB Insights*, No. 18(1).

[35] Jarrahi, M.H., 2018. Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making, *Business Horizons*, No. 61(4).

[36] Jormanainen, I., Koveshnikov, A., 2012. International Activities of Emerging Market Firms A Critical Assessment of Research in Top International Management Journals, *Management International Review*, No. 52.

[37] Kaplan, A., Haenlein, M., 2019. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence, *Business Horizons*, No. 62(1).

[38] Karppi, T., 2018. "The Computer Said So": On the Ethics, Effectiveness, and Cultural Techniques of Predictive Policing, *Social Media + Society*, No. 4(2).

[39] Kietzmann, J., Pitt, L.F., 2020. Artificial intelligence and machine learning: What managers need to know, *Business Horizons, Artificial Intelligence and Machine Learning*, No. 63(2).

[40] Kitsios, F., Kamariotou, M., 2021. Artificial intelligence and business strategy towards digital transformation: A research agenda, *Sustainability*, No. 13(4).

[41] Koch, R., 2019. *What is considered personal data under the EU GDPR?*, https://gdpr.eu/eu-gdpr--personal-data/ (10.06.2021).

[42] Königstorfer, F., Thalmann, S., 2020. Applications of Artificial Intelligence in commercial banks – A research agenda for behavioral finance, *Journal of Behavioral and Experimental Finance*, No. 27.

[43] Kop, M., 2021. *E.U. Artificial Intelligence Act: The European Approach to AI. Vol. 2*, Stanford University.

[44] Kornai, J., 2008. *The Great Transformation of Central Eastern Europe: Success and Disappointment*, [in:] Kornai, J., Mátyás, L., Roland, G. (eds.), *Institutional Change and Economic Behaviour. International Economic Association Series*, Palgrave Macmillan.

[45] KPMG, 2018. *Many Companies Are Not Assessing Risks Of Adopting Emerging Technologies: KPMG Study*, https://www.proquest.com/wire-feeds/many-companies-are-not-assessing-risks-adopting/docview/1995233718/se-2?accountid=15539 (02.05.2021).

[46] Kurzweil, R., 2013. How to create a mind: The secret of human thought revealed, Penguin.

[47] Lee, M.K., 2018. Understanding perception of algorithmic decisions: Fairness, trust, and emotion in response to algorithmic management, *Big Data & Society*, No. 5(1).

[48] Loureiro, S.M.C., Guerreiro, J., Tussyadiah, I., 2021. Artificial intelligence in business: State of the art and future research agenda, *Journal of Business Research*, No. 129.

[49] Lu, Y., 2019. Artificial intelligence: A survey on evolution, models, applications and future trends, *Journal of Management Analytics*, No. 6(1).

[50] Madiega, T.A., 2021. *Artificial intelligence act*, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792 (22.10.2021).

[51] Meyer, K.E., Peng, M.W., 2005. Probing theoretically into Central and Eastern Europe: Transactions, resources, and institutions, *Journal of International Business Studies*, No. 36(6).

[52] Meyer, K.E., Peng, M.W., 2016. Theoretical foundations of emerging economy business research, *Journal of International Business Studies*, No. 47(1).

[53] Morel, B., 2011. Artificial intelligence and the future of cybersecurity, *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, October.

[54] Ng, A., 2016. *AI Winter Isn't Coming*, https://www.technologyreview.com/2016/12/07/155592/ai-winter-isnt-coming/ (17.03.2020).

[55] OECD, 2021. *The Digital Transformation of SMEs, OECD Studies on SMEs and Entrepreneurship*. Paris: OECD Publishing.

[56] Ozkan, B.Y., Spruit, M., 2021. *Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda*, [in:] *Research Anthology on Artificial Intelligence Applications in Security*, IGI Global.

[57] Patel, F., 2015. *Be Cautious About Data-Driven Policing*, https://www.nytimes.com/roomfordebate/2015/11/18/can-predictive-policing-be-ethical-and-effective/be-cautious-about-data-driven-policing (22.06.2021).

[58] PwC, 2022. *Entrepreneurship and SMEs*, https://www.pwc.com/c1/en/future-of-government-cee/entrepreneurship-and-smes-in-CEE.html (06.05.2021).

[59] Rupeika-Apoga, R., Bule, L., Petrovska, K., 2022. Digital Transformation of Small and Medium Enterprises: Aspects of Public Support, *Journal of Risk and Financial Management*, No. 15(2).

[60] RUSSELL, S.J., NORVIG, P., 2020. *Artificial intelligence: A modern approach. Prentice-Hall series in artificial intelligence (4th ed.)*, Upper Saddle River: Prentice-Hall.

[61] SELBST, A.D., POWLES, J., 2017. Meaningful information and the right to explanation, *International Data Privacy Law*, No. 7(4).

[62] ȘERBAN-OPRESCU, G.L., 2019. Digitalization and business activity. The struggle to catch up in CEE countries, *Sustainability*, No. 11(8).

[63] SOULSBY, A., CLARK, E., 2007. Organization theory and the post-socialist transformation: Contributions to organizational knowledge, *Human Relations – HUM RELAT*, No. 60.

[64] STRAUB, J., 2021. Expert system gradient descent style training: Development of a defensible artificial intelligence technique, *Knowledge-Based Systems*, No. 228.

[65] STUURMAN, k, LACHAUD, E., 2022. Regulating AI A label to complete the proposed Act on Artificial Intelligence, *Computer Law & Security Review*, No. 44.

[66] TADDEO, M., MCCUTCHEON, T., FLORIDI, L., 2019. Trusting artificial intelligence in cybersecurity is a double-edged sword, *Nature Machine Intelligence*, No. 1(12).

[67] TRAȘCĂ, D., STEFAN, G., SAHLIAN, D., VAN HOINARU, R., SERBAN-OPRESCU, G., 2019. Digitalization and Business Activity. The Struggle to Catch Up in CEE Countries, *Sustainability*, No. 11.

[68] TUTAK, M., BRODNY, J., 2022. Business Digital Maturity in Europe and Its Implication for Open Innovation, *Journal of Open Innovation: Technology, Market, and Complexity*, No. 8(1).

[69] VĂTĂMĂNESCU, E.-M., ANDREI, A.G., NICOLESCU, L., PÎNZARU, F., ZBUCHEA, A., 2017. The Influence of Competitiveness on SMEs Internationalization Effectiveness. Online versus Offline Business Networking, *Information Systems Management*, No. 34(3).

[70] VĂTĂMĂNESCU, E.-M., GORGOS, E.-A., GHIGIU, A.M., PĂTRUȚ, M., 2019. Bridging Intellectual Capital and SMEs Internationalization through the Lens of Sustainable Competitive Advantage: A Systematic Literature Review, *Sustainability*, No. 11(9).

[71] WAGNER, B., 2019. Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems, *Policy & Internet*, No. 11(1).

[72] WHITLEY, R., CZABAN, L., 1998. Institutional transformation and enterprise change in Hungary, *Organization Studies*, No. 19(2).

[73] WORLD BANK, 2022. *SME Finance*, https://www.worldbank.org/en/topic/smefinance (10.02.2022).

[74] YUDKOWSKY, E., 2008. Artificial intelligence as a positive and negative factor in global risk, *Global catastrophic risks*, No. 1(303).