SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 212

LEGAL LIABILITY OF AN ORGANISATION USING ARTIFICIAL INTELLIGENCE

Szymon RUBISZ

Silesian University of Technology; szymon.rubisz@polsl.pl, ORCID: 0000-0002-0999-5855

Purpose: an analysis of the impact of artificial intelligence on organisations, with a particular focus on the legal liability associated with the use of AI-based tools.
Design/methodology/approach: legal and qualitative analysis of AI's impact on organizations, focusing on general principles of civil law and regulatory frameworks like the AI Act. The paper adopts a formal-dogmatic method of interpreting legal texts and case-study approach, examining specific instances of AI use, and covers theoretical aspects of liability, data privacy, intellectual property etc.
Findings: the analysis reveals that while AI greatly enhances efficiency and innovation, it also introduces complex legal risks, particularly concerning data privacy, liability, and intellectual property. In many cases, existing rules and laws may be adequate to deal with potential infringements using AI. The EU legislation being implemented provides for new specific obligations for AI operators complementing existing spheres of legal liability. Due to the legal uncertainty, organisational managers have to balance efficiency and accountability.
Originality/value: an analysis of the impact of artificial intelligence (AI) on the legal liability of organisations, particularly in the context of civil and administrative law (within EU). The paper highlights AI as a key tool in organisations, but also identifies legal risks due to the lack of national legislation specific to AI. It is intended for decision-makers implementing AI within organisations.

Keywords: legal liability, artificial intelligence, organizations liability.
Category of the paper: research paper.

1. Introduction

Artificial intelligence (AI) has rapidly become the technology backbone of many modern organisations, revolutionising various aspects of business conduct and decision-making. Its importance is underlined by its ability to increase productivity, innovation, and competitive advantage across industries (Holmström, 2022). However, this technological phenomenon carries a number of potential risks. Fundamentally, this is because it is not an 'entity' that thinks and rationalises its 'decisions', it acts in a way that is delineated by its creator but not necessarily

http://dx.doi.org/10.29119/1641-3466.2024.212.29

fully anticipated and controlled by him, autonomously adapting to new situations in many situations (Yampolskiy, 2024). As such, it can be an agent of damage and harm to other entities, especially private individuals, and thus the question arises as to who and what legal liability is incurred in this respect.

Even though AI has been accompanying humanity in practical terms for several years now, the issue of legal liability is still unsolved. There are also relatively few scientific studies on this topic, and journalistic and popular science texts predominate. A frequent feature of legal provisions is their lack of relevance to new technological phenomena due to the slow reaction of legislators. This raises the problem of the multiplicity of interpretations and approaches in situations not explicitly resolved by the norms. The aim of this article is therefore to identify the areas and scope of liability of an organisation using artificial intelligence algorithms. The paper is a prelude to further in-depth research into legal liability within specific branches of law based on analyses of legal acts and court judgments. These are few for the time being, but the regulation of this area, which is new to the legal system and the judiciary, is certainly to be expected in the future. Further considerations are based on the interpretation of general principles of law and an attempt to juxtapose them with possible infringements in connection with the application of AI but without reference to the content of specific state laws and acts. The whole is complemented by a general overview of the proposals and framework regulations adopted in the European Union, which are the first in the world to attempt to create a catalogue of the obligations of AI operators and the consequences of failing to comply with them. Therefore, the formal-dogmatic method, typical of the legal sciences, will be applied here. The above remarks lead one to conclude that such an analysis is needed and can be a valuable resource for organisational managers, and this article aims to contribute to this.

2. The concept and relevance of AI for modern organisations

The term ‘artificial intelligence’ has still not arrived at a uniform, universally accepted definition. In general, it is a field of computer science that studies methods and software that enable machines to perceive their environment and use knowledge and intelligence to take actions that maximise their chances of achieving specific goals (Russel, Norvig, 2021). Attempts to determine the meaning of the term have been made since the mid-20th century with varying degrees of intensity, depending on the various approaches and levels of technological development (Kumalski, 2022). It is not the purpose of this paper to present various definitions of the term AI; a broad overview of these is presented by Russel and Norvig (2021). For this thesis, it can be assumed that AI is an information system that suggests solutions to the problems posed to it based on data collected by it (machine learning), analysed, logically processed along the lines of human reasoning, and presented to the user in a comprehensible (natural language) and desirable form (text, image, sound, et al.). Implementing such a system can refer to an application accessible through a computing device, as well as being a component of a self-functioning machine, such as an autonomous vehicle.

The pioneer to mention a ‘thinking machine’ is believed to have been Alan Turing (1950), while the term ‘Artificial Intelligence’ was coined by John McCarthy (Aziz, 2023). In the mid-twentieth century, the construction of such machines was only a matter of futurology. In recent years, however, AI has reignited people's minds. Thanks to the gigantic amount of data stored in the memories of computers and global access to them via the Internet, as well as the enormous computing power of modern processors, it has become possible and obvious to create tools with which humans can somehow make use of these unimaginable resources in an efficient, synthetic, but also economical way considering, for example, the time and cost of information processing. Computer systems today are no longer simple programs performing automated, obvious, and relatively simple (but still useful) tasks. AI can successfully serve and is already being used in many areas of life, e.g. content generation in the creative and entertainment industries, electronic diagnosis of human diseases or malfunctions in machines, air or sea traffic control, automatic assessment of the creditworthiness of borrowers, in education, customer service, and these are just some examples of ever-evolving applications. Undoubtedly, artificial intelligence also plays an increasingly important role in modern organisations, influencing various aspects of business operations, decision-making, and strategic planning.

One of the most profound impacts of artificial intelligence is its ability to automate routine tasks, thereby increasing operational efficiency. AI-enabled tools and systems can fulfil a variety of functions, from customer service chatbots to robotic process automation for repetitive office tasks such as data retrieval, form filling and so on. By automating repetitive and basic duties, an organisation can direct employees' attention to other strategic, innovative and more rewarding endeavours, ultimately increasing productivity and reducing operational costs (Davenport et al., 2023; Morandini et al., 2023; Lukan, 2024).

In the age of big data, artificial intelligence plays a key role in transforming raw information into useful information. Advanced algorithms can analyse huge data sets to identify patterns, trends and anomalies that a human would not be able to access on their own. This capability enables companies to make more informed choices, optimise business processes and predict trends with greater accuracy (Duan et al., 2019). For example, AI-based predictive analytics can help companies predict customer needs and behaviour or build strategies (Law, 2024).

AI is a key driver of innovation in contemporary organisations. Using artificial intelligence, companies can develop new products, offerings and business models. It is enough to pay attention to the services that have long been available on the market using complex, intelligent algorithms. For example, artificial intelligence is influencing the automotive industry through the increasing autonomy of the vehicle and the ‘smart’ sensors operating within it (Rudkovska, 2023); the services offered by various providers to recognise products, objects or places from photos, voice assistants, tools using generative AI, et al. (Uzialko, 2024).

Algorithms are revolutionising the way businesses interact with their customers. With artificial intelligence-based, self-updating customer relationship management (CRM) tools, organisations can anticipate customer needs and expectations. A. Uzialko (2024) gives the example of a service from a certain bank that notifies a borrower to pay the next instalment when the borrower is near a branch of that bank. Taking this a step further, organisations can respond to queries in real time because, available 24/7, chatbots and virtual assistants can provide information and assistance more and more efficiently and effectively, increasing customer satisfaction and loyalty. What's more, artificial intelligence can analyse customer comments and sentiments to improve its products and services, to profile its audience and provide them with products that best fit their preferences (e.g. music and movie recommendations from streaming services).

Artificial intelligence is undeniably a transformative force in today's organisations. Its ability to increase operational efficiency, support data-driven decision-making, foster innovation and improve the customer experience, and ultimately gain competitive advantage, makes it an essential tool for companies across industries. The business benefits seem enormous, but companies also face legal challenges. The use of AI in business, like any other tool, involves potential infringement of the interests of others, e.g. personal rights, privacy or personal data; it is a threat of formal errors, e.g. in accounting records; and finally, it is a possible tort of criminal law. Awareness of the areas of legal liability and limitations in the use of AI is essential to ensure that business does not suffer the negative consequences of possible illegal actions, including loss of customer trust.

3. Legal liability of the organisation

The legal system generally distinguishes three basic types of liability: civil, administrative and criminal. There are also other forms of liability, such as labour, disciplinary or statutory, but these are variations of the aforementioned categories. Each entails specific sanctions: civil and administrative usually result in the payment of a sum of money as compensation (which has a compensatory rather than a punitive function) or an administrative fine, while criminal may lead to a criminal penalty, such as imprisonment. The latter, however, is individual in nature and thus applies to a specific person, e.g. a manager for a crime committed. Although many national legislations provide for the institution of liability of a collective entity, the conduct of criminal proceedings is most often linked to the prior conviction of a specific individual. In contrast, the liability of the organisation itself is reduced to a financial sanction covered by its assets. For this reason, the issue of criminal liability will be disregarded in the remainder of this paper. Although it is worth emphasising that in various situations of AI use, typically civil law claims against an organisation may be accompanied by criminal charges against individual individuals associated with the organisation.

3.1. Civil liability

Civil liability relates to the sphere of legal relations between private civil law entities, i.e. natural persons, legal persons or other organisational entities that are not legal persons but to which the law has granted legal subjectivity. It should be noted that each of these types of entities can be identified with an organisation, depending on the legal form adopted by its creator. Civil liability can be either tortious, i.e. related to the commission of a tort, or contractual concerning the non-performance or improper performance of a contract.

The emergence of civil liability in tort is the result of three cumulative conditions being met. Firstly, the occurrence of conduct, i.e. the act or omission of the entity that led to the damage. In the context of AI, one can point to, for example, the machine learning stage, when an algorithm extracts data from sources protected by, for example, copyright. Another example relates to the generation of sound or images that may infringe someone's physical or auditory image. Secondly, the occurrence of damage, i.e. harm to legally protected goods and interests, which may be material (property, the extent of which can be expressed economically, e.g. plagiarism, accident involving an autonomous vehicle, errors in the financial system) or immaterial (non-material, affecting the goods and interests of the victim but not translating into the victim's property, e.g. violation of personal rights, privacy, discrimination, generation of false information). Thirdly and finally, there must be a causal link between the event and the damage, as liability is only incurred for the normal consequences of the act or omission from which the damage arose. The attribution of liability for damages is, of course, possible concerning the one to whom fault can be attributed. In most cases, it is irrelevant whether the fault is intentional (intention to cause damage or harm) or unintentional (lack of intention, carelessness of action). Instead, what is relevant is whether the act in question is unlawful, i.e. whether it violates the applicable legislation and, in some legislations, also the principles of social co-existence. Such an assessment is usually made by the court at trial, but regardless of this, the aggrieved party always has the right to lodge a claim against the perpetrator. In the context of the use of artificial intelligence, it would therefore have to be verified whether the effect of its action is indeed an unlawful act under the relevant legislation and, if so, whether someone can be attributed fault. If this cannot be done, no one will be held legally responsible, even if the damage occurred.

3.2. Administrative liability

Another type of liability is administrative liability, which stems from administrative laws that regulate the relationship between public authorities and other subjects of the law. This branch of law is highly dependent on the political and legal system adopted in a given national legislation, specific local rules or traditions. It is, therefore, difficult to identify a catalogue of principles of legal liability in this area that would be universally applicable. Another difficulty is that there is no unambiguous set of rules defining sanctions for violations of administrative law due to the vastness and diversity of the scope of regulation, for example, covering tax law, environmental law, social welfare and others.

In contrast, it can be said that administrative liability is mainly repressive in nature, and its purpose is to compel the performance of administrative duties. It is objective in nature, which means that it does not depend on the intentional or unintentional fault of the perpetrator unless the provision so indicates. The breach of the provision itself is decisive. Sanctions for violations of administrative law can be both monetary and non-monetary. Financial sanctions include various types of administrative fines and fees. Non-financial sanctions, on the other hand, may include obligations of specific behaviour, such as an order to demolish a building or stop the operation of an establishment.

4. Areas of liability for the use of AI

4.1. Areas of potential infringements

The possibilities outlined at the beginning of this thesis, offered to organisations by the use of artificial intelligence, show that it is undoubtedly a phenomenon that will develop and will become increasingly widespread. At the same time, it seems necessary to identify areas where there could potentially be breaches of existing law. It might be wrong to believe that a specific technological innovation is something unprecedented and unique, that it completely escapes the existing legal rules that have not kept up with technological progress. It's because it turns out that we are dealing with virtually the same consequences indicated in the legislation, i.e. the occurrence of certain events or behaviour resulting in damage or harm. However, it is achieved using a new tool, in this case artificial intelligence, but this, from the point of view of existing legal provisions, should be irrelevant in many cases. Therefore, it is possible to identify various legally regulated areas in which infringements caused by the use of artificial intelligence systems may occur.

First of all, it is worth mentioning human personal rights in its broadest sense. These are collectively accepted in a given culture, non-material values relating to a person's physical and mental integrity, dignity and position in society (Radwański, 2007; Bojanowski, 2023). These can include such universal values as health, freedom, dignity, good name, privacy or image. It is not difficult to imagine threats to personal goods when they come into contact with systems equipped with artificial intelligence algorithms.

A related example of personal rights is certainly the issue of IT system processing of sets of information about individuals - personal data and sensitive information concerning health, sexual orientation, political opinions or religion. The source of such data may be social media, where users build a profile by filling it with information about themselves, photos, statements and others. A source of valuable information may be a bot with which the user ‘talks’ as if it were a human being. The data collected in this way serves a variety of needs for different organisations, ranging from the typically business-related, e.g. to address marketing messages, to criminal purposes for fraud, phishing, impersonation or the spread of hate speech. In the EU, personal data is subject to protection requirements under the GDPR regardless of how it is collected, processed or stored. Compliance with EU regulations requires controllers of personal data to demonstrate the necessity and appropriateness of the extent of data collected, while AI systems need vast amounts of data to operate and grow. In addition, it is necessary to inform the data owner of the purposes and means of data processing, as well as to obtain their consent to the processing. Meanwhile, the functioning of an AI system, the level of complexity of the actions it takes and the results it produces may not be predictable or even comprehensible to the controller itself. There is also no certainty that AI will only use the information for the purpose assumed by the controller. Therefore, precise and complete information for the data owner, and consequently his consent expressed with full awareness, may be difficult to achieve (Chalubinska-Jentkiewicz, Nowikowska, 2022). In this context, it is worth mentioning the complaint of the organisation NOYB against OpenAI to the Austrian data protection authority regarding the inability of the ChatGPT algorithm (OpenAI's product) to correct the data collected on the person represented by the complainant. OpenAI was unable to comply with the obligations imposed on it by the GDPR (requesting deletion or correction of data), and an inspection procedure was initiated as a result of this breach (NOYB, 2024).

The need to comply with the requirements of GDPR is only the beginning of the problems that may arise in relation to AI processing of information about individuals. There may be doubts related to possible errors in profiling these individuals. It may result in making the wrong decision regarding specific characteristics or abilities of a given person, e.g. in the recruitment process (Czajkowski, Stroińska, 2023), whereby allegations of discrimination and bias become possible. Going further, the privacy of data subjects should be a concern. It may be that artificial intelligence tools infer sensitive information, such as political views or health status, from seemingly innocuous and unrelated data. This was demonstrated by the example of Cambridge Analytica, which, by running millions of inconspicuous personality quizzes on Facebook, created a campaign of personalised election ads ahead of the 2016 US presidential election (Sullivan, 2023).

Also linked to privacy and personal rights is, of course, the issue of a person's image, which is usually an image of a face, voice or other features by which that person can be identified. Generative AI can create both a realistic image and voice of a person, whether actually existing or completely invented. In the former case, the algorithm 'learns' the appearance, behaviour, facial expressions and intonation of a particular person from available photos and audio and video recordings. At this point, it is worth recalling the high-profile case in which actress Scarlett Johansson accused OpenAI that its new voice assistant sounds strikingly similar to her voice. It should be noted that the artist had previously rejected the offer to lend her voice. The company argued that the voice belonged to another actress, but the assistant was eventually switched off (Milmo, 2024). When an algorithm creates an image of a non-existent person, it does so using collections of facial images of people who actually exist. For example, IBM used nearly one million photos from Flickr, a popular photo-sharing platform, to train its facial recognition software without the explicit consent of the people in the photographs. The company argued that the photos were publicly available, but it should be noted that the photos were originally shared on Flickr for a different purpose (Sullivan, 2023).

Another area of consideration for AI legal liability is its use in the field of intellectual property. In creative and inventive activities, the possibilities of AI are extraordinary and innumerable: from suggesting creative ideas, to proposing forms and main elements of content to generating ready-made and attention-grabbing unique images, films, musical, literary works or computer programs. However, both in the context of copyright and invention law, certain doubts arise, which will only be indicated here. Firstly, the question of the novelty of the creative effect - AI tools, for the time being, do not create entirely new ideas on their own, but only support human creativity (Bieser, 2022). Algorithms generate their realisations based on analysed, ubiquitously available ready-made creations, many of which have probably been created by humans in a creative process and are covered by exclusive rights. This raises the issue of whether such exploitation should be regarded as an encroachment on the exclusive rights of creators, publishers and producers and, therefore, as infringement, or whether it can be likened to a human information acquisition or technological process and covered by an appropriately worded statutory licence (Torrance, Tomlinson, 2023; Geiger, Iaia, 2024). Within the framework of European Union law, it has been accepted that the exploitation of intellectual property for the purposes of machine learning (text and data mining) may be prohibited by express reservation by the right holder. However, in the absence of such a reservation, it is allowed as one of the forms of permitted use without having to obtain a separate authorisation (Art. 4 DSM, 2019).

Secondly, whether the creations generated by AI can be protected by exclusive rights (i.e. whether they constitute works within the meaning of copyright law or whether they can be patentable inventions) and, if so, who will be their possessor: the AI, its creator or the prompting person. In this respect, the laws of most countries make it clear that the rights holder can only be a human being. However, it is not always clear how to treat the situation where generative AI contributes to the creative or inventive process, whether this contribution is minimal or significant. In the US, for example, it is excluded to include artificial intelligence as a co-inventor (Vidal, 2024). EU and UK law regulate it in the same way, while on the other hand, the Canadian Intellectual Property Office has recently listed the DABUS application as an inventor in a patent document (Di Piano, 2024). In conclusion, current legislation does not allow to prejudge with certainty the status of intellectual property created by AI. Arguably, the general premise of this branch of law of creative human involvement in the process should be used. The extent of this involvement should be decisive for the granting of protection, and where it is minimal or non-existent, the generated product should be considered part of the public domain. However, the evidentiary process can be extremely difficult here, as it will rely heavily on the declarations of the entity interested in protection. Thus, the use of such creations of uncertain status by others, will be risky and may expose them to legal liability.

In the context of accountability for the use of AI, the issue of access to and use of information certainly cannot be overlooked. The use of AI-based tools in market analysis and economic forecasting can serve as an example here. Patterns and relationships identified by the algorithm may generate benefits, but suggesting them, basing future investment decisions and advice on them, is undoubtedly a risk. This is because even inferring future trends from historical data by AI is a risk. Here, the algorithm may generate misleading forecasts without taking into account unexpected political events, economic crises, and natural disasters (Rane et al., 2024). At the same time, the tool user would have no insight into how it arrived at its recommendations (the ‘black box’), whether it relied on erroneous data, or confabulated, resulting in misinterpretations and wrong decisions (Yalamati, 2023). The question of legal liability in this regard would primarily concern the breach of contractual obligations and the triggering of disciplinary clauses and contractual penalties for material damage caused. The above considerations are also not difficult to apply *per analogiam* to the advice given by lawyers, doctors or tax advisers. In the case of these professions, not only contractual liability will come into play, but also disciplinary liability within their professional organisations.

Staying on the subject of information and artificial intelligence, the problem of disinformation using fake news, deepfake etc. cannot be overlooked. The motivation for their use is economic or political gain, or the intention to deceive or harm another person or business. The multitude and ease of use of available AI tools for modifying statements using someone else's voice, adjusting lip movements to it, generating videos with other people's images, and generating misleading opinions and assessments about competitors – these are just some of the examples of applications of artificial intelligence algorithms. The basis for legal liability in this respect will be sought in the provisions of civil law on the protection of personal rights, as already mentioned above, in relation to infringements of reputation, dignity, privacy or image. However, we should also mention that e.g. in Polish law, criminal provisions provide for the offences of defamation and insult, generally prosecuted by private prosecution.

4.2. The issue of the subject of liability

When considering issues of legal liability arising from the use of artificial intelligence, we are first confronted with the momentous problem of determining who is liable. In the case of existing algorithms, this has not really been a dilemma, as liability could, in principle, be attributed to the person who used the computer program or device in question, or alternatively to the manufacturer of the software if the resulting damage was caused by its errors. However, the situation is somewhat different when dealing with algorithms that operate completely or largely autonomously and independently of human oversight (the ‘black box’ principle); it is not fully known what effect new data fed into such a system has on it; the source codes of the algorithms are generally legally protected and rather secret. Consequently, accountability is somewhat diluted.

Liability cannot be attributed to artificial intelligence, given the aforementioned aspect of guilt, which, after all, can only be attributed to humans. After all, neither the machine nor the software controlling it has legal subjectivity. It is also difficult to accept that no one is responsible for the damage or harm caused, as is the case with so-called force majeure or damage caused by wild animals. Attention should, therefore, be directed at the artificial intelligence operator providing both the tool and the infrastructure for potential violations. In some jurisdictions, the legitimacy of claims could be sought in product liability laws (strict liability), although in this respect, Polish law, for example, only provides for the physical form of such a product, which obviously excludes artificial intelligence. The problem was noticed by the European Union authorities, who, as a result of several years of work, adopted Regulation 2024/1689, commonly referred to as the AI Act. The regulations do not cover the private use of AI by individuals but are primarily aimed at those who create and market such systems in the EU, i.e. providers, importers and distributors. In addition to them, deployers, i.e. organisations implementing and using AI systems in practice in their business operations, are also identified.

The aim of the regulation is, on the one hand, to provide clear guidelines for creators to develop their solutions and, on the other hand, to guarantee individuals an adequate level of protection of their rights (Stawicka, 2024). AI systems are classified into four categories of risk levels: unacceptable (prohibited creation and use), high, limited and minimal (none). The highest risk level relates to AI used to capture extremely sensitive data, and therefore, any processing of health, biometric, opinion or behavioural data will be prohibited. Systems with a lower level of risk are allowed, albeit subject to regulatory requirements. For adopters, it will be mandatory to implement appropriate technical and organisational measures to use AI systems in accordance with their instructions; to keep automatically generated logs of AI systems, if under control, for a certain period of time; to carry out an assessment of the impact on fundamental rights by adopters of high-risk AI systems, especially when providing essential public services, before using them for the first time. This protection is to be further strengthened by the transparency of generative AI models, i.e. the need for them to meet certain standards before they are marketed. Violations of the Regulation by obliged entities will result in fines of up to €35 million and, if the violator is a company, up to 7% of its annual global turnover (Rytel, 2024).

Independently of the AI Act, legislative solutions for civil liability are also in the pipeline in the EU. They are to concern non-contractual claims leaving aside contractual liability, where the general principles of freedom of contract remain sufficient. They aim to harmonise, using a directive, the rather diverse national regulations in this area, which are not conducive to the development of the common market (Skibińska, 2022). Liability is to be borne by the operators, i.e. the persons designing the system or entering data into it, who have control over it, which translates into a level of risk for those using it. More specifically, a presumption of operator fault would be introduced for damage caused by high-risk AI. The defendant, on the other hand, would have to rebut this presumption to avoid consequences such as compensation. In terms of the concepts used, the provisions of the Directive are intended to refer to the AI Act, so that an operator is to be understood as both the one who creates the algorithm, markets it and the one who uses tools based on it.

4.3. The need for balance

As artificial intelligence becomes increasingly integrated into business operations, companies face the challenge of balancing the benefits of these tools with the responsibility and legality of data use. Striking this balance is critical for maintaining trust, avoiding legal complications, and unlocking AI's potential responsibly. Businesses should understand and comply with regulations – staying informed about laws and other industry-specific regulations is essential. Companies should establish a robust data governance framework to ensure compliance, incorporating privacy-by-design principles to make privacy an integral part of AI development. Another issue is the ethical acquisition and use of data and the need for transparency. The data should be collected with informed, explicit consent, ensuring users understand how their data will be used. Appropriate security measures concerning privacy should also be ensured. To ensure AI systems remain trustworthy, companies should regularly audit algorithms for compliance, accuracy, and bias. Maintaining detailed logs of data usage and processing ensures accountability while verifying that third-party tools meet ethical and legal standards is equally important. Moreover, employees must be trained on data privacy laws, ethical AI principles, and best practices for handling sensitive information. Cultivating a culture that prioritizes ethical responsibility ensures alignment across the organization. Navigating the complexities of data protection laws and ethical AI use is challenging. Consulting legal experts ensures compliance, while working with ethics consultants helps align AI initiatives with societal values and expectations. By implementing these strategies, businesses can successfully balance the innovative capabilities of AI with the responsibility and legality of data use. This approach not only ensures regulatory compliance but also builds trust among stakeholders, creating a foundation for long-term success.

5. Conclusion

This paper is intended as an introduction to an in-depth study of AI liability based on the provisions of various branches of law. The analysis presented here is necessarily cursory and overview-based. At the same time, it is useful in identifying areas and potential problems and in helping to select provisions that may be applicable in specific cases, thus providing a valuable resource for the organisation's managers.

From the above analysis, it is clear that the development of artificial intelligence undoubtedly opens up an extremely wide range of opportunities for organisations, with its ability to automate processes, analyse large sets of data, contribute to innovation, efficiency and gain competitive advantage. But it also poses legal liability challenges concerning privacy, personal data, intellectual property or the generation of disinformation. These and other areas of responsibility have been identified as crucial.

Secondly, the adoption of legislation such as the AI Act in the EU is a first step towards regulating the AI market, aiming not only to formulate principles of responsibility for the creation and use of tools, but also to protect the rights of individuals. However, it is important to bear in mind that, despite the Regulation coming into force in mid-2024, it requires implementation in EU member states, and this is expected to take place over the next two years. Some provisions have an even longer *vacatio legis* of 36 months. The directive on civil liability, on the other hand, is still at the drafting stage.

And finally, for the time being, it is only possible to anticipate how these regulations will be applied, what impact they will have on organisations – those providing and those deploying, and what stage of development artificial intelligence itself will be at in two years. Until then, infringements of others' rights caused by the use of AI systems must be treated in the same way as they happen when they occur in other situations, according to current laws and rules. Ultimately, organisations will have to balance efficiency with accountability.

References

1. Aziz, A. (2023). Artificial Intelligence Produced Original Work: A New Approach to Copyright Protection and Ownership. *European Journal of Artificial Intelligence and Machine Learning, Vol. 2, No. 2,* pp. 9-16, doi: 10.24018/ejai.2023.2.2.15.
2. Bieser, J. (2022). Creative through AI: How artificial intelligence can support the development of new ideas. *Gottlieb Duttweiler Institute Research Paper, No. 4610307.* Retrieved from: https://dx.doi.org/10.2139/ssrn.4610307, 10.10.2024.

3. Bojanowski, T. (2023). Mowa nienawiści a dobra osobiste – wybrane aspekty ochrony cywilnoprawnej. *Annales Universitatis Mariae Curie-Skłodowska Lublin – Polonia, Vol. LXX, Iss. 1*, pp. 23-37, doi: 10.17951/g.2023.70.1.23-37.
4. Chałubińska-Jentkiewicz, K., Nowikowska, M. (2022). Artificial Intelligence v. Personal Data. *Polish Political Science Yearbook, Vol. 51, Iss. 3*, pp. 183-191, doi: 10.15804/ppsy202240.
5. Czajkowski, E., Stroińska, J. (2023). *Jakie ryzyka niesie za sobą rekrutacja z pomocą AI.* Retrieved from: https://pro.rp.pl/kadry-i-place/art39488371-jakie-ryzyka-niesie-za-soba-rekrutacja-z-pomoca-ai, 10.10.2024.
6. Davenport, T.H., Holweg, M., Jeavons, D. (2023). *How AI Is Helping Companies Redesign Processes.* Retrieved from: https://hbr.org/2023/03/how-ai-is-helping-companies-redesign-processes, 10.10.2024.
7. Di Piano, N. (2024). *Ghost in the machine: AI and patent protection*. Retrieved from: https://www.smartbiggar.ca/insights/publication/ghost-in-the-machine--ai-and-patent-protection, 10.10.2024.
8. Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130 from 17.5.2019, pp. 92-125 (2019).
9. Duan, Y., Edwards, J.S., Dwivedi, Y.K. (2019). Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda. *International Journal of Information Management, Vol. 48*, pp. 63-71, doi: 10.1016/j.ijinfomgt.2019.01.021.
10. Geiger, C., Iaia, V. (2024). The Forgotten Creator: Towards a Statutory Remuneration Right for Machine Learning of Generative AI. *Computer Law & Security Review, Vol. 52*, *No. 105925*, doi: 10.1016/j.clsr.2023.105925.
11. Holmström, J. (2022). From AI to digital transformation: The AI readiness framework. *Business Horizons*, *Vol. 65, Iss. 3*, pp 329-339, doi: 10.1016/j.bushor.2021.03.006.
12. Kumalski, K. (2022). Sztuczna inteligencja jako instrument intensyfikacji zagrożeń hybrydowych w domenie informacyjnej. *Sprawy Międzynarodowe*, *Vol. 75, No. 2,* pp. 93-123, doi: 10.35757/sm.2022.75.2.06.
13. Law, M. (2024). *AI-Powered Predictive Analytics Driving Business Success*. Retrieved from: https://technologymagazine.com/articles/ai-powered-predictive-analytics-driving-business-success, 10.10.2024.
14. Lukan, E. (2024). *How AI process automation revolutionizes operations management*. Retrieved from: https://www.synthesia.io/learn/ai-applications/process-automation, 10.10.2024.
15. Milmo, D. (2024). *Scarlett Johansson's OpenAI clash is just the start of legal wrangles over artificial intelligence.* Retrieved from: https://www.theguardian.com/technology/article/2024/may/27/scarlett-johansson-openai-legal-artificial-intelligence-chatgpt, 10.10.2024.

16. Morandini, S., Fraboni, F., De Angelis, M., Puzzo, G., Giusino, D., Pietrantoni, L. (2023). The Impact of Artificial Intelligence on Workers' Skills: Upskilling and Reskilling in Organisations. *Informing Science: The International Journal of an Emerging Transdiscipline, Vol. 26,* pp. 039-068, doi: 10.28945/5078.
17. NOYB (2024). Retrieved from: https://noyb.eu/en/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it, 10.10.2024.
18. Radwański, Z. (2007). *Prawo cywilne – część ogólna*. Warszawa: C.H. Beck.
19. Rane, N., Mallick, S.K., Kaya, Ö., Rane, J. (2024). Applications of machine learning in healthcare, finance, agriculture, retail, manufacturing, energy, and transportation: A review. In: N. Rane, Ö. Kaya, J. Rane, *Applied Machine Learning and Deep Learning: Architectures and Techniques* (pp. 112-131). Deep Science Publishing.
20. Rezolucja Parlamentu Europejskiego z dnia 20.10.2020 r. z zaleceniami dla Komisji Europejskiej w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję, 2020/2014(INL), Dz.U. C 404 z 6.10.2021, pp. 107-128.
21. Rudkovska, O. (2023). *AI in Transportation: Common Use Cases Shaping the Industry.* Retrieved from: https://euristiq.com/ai-in-transportation/, 10.10.2024.
22. Russell, S.J., Norvig, P. (2021). *Artificial Intelligence: A Modern Approach (4th ed.).* Hoboken: Pearson, pp. 1-4.
23. Rytel, A. (2024). *AI Act ureguluje zasady korzystania ze sztucznej inteligencji.* Retrieved from: https://www.prawo.pl/biznes/ai-act-zasady-korzystania-ze-sztucznej-inteligencji,526385.html, 10.10.2024.
24. Skibińska, R. (2022). *Odpowiedzialność za sztuczną inteligencję będzie uregulowana.* Retrieved from: https://www.prawo.pl/biznes/odpowiedzialnosc-za-sztuczna-inteligencje-beda-przepisy,517822.html, 10.10.2024.
25. Stawicka, I. (2024). *AI Act wkrótce zmieni firmową rzeczywistość – warto się już przygotowywać.* Retrieved from: https://www.prawo.pl/biznes/ai-act-obowiazki-dla-firm,525932.html, 10.10.2024.
26. Sullivan, M. (2023). *Examining Privacy Risks in AI Systems*. Retrieved from https://transcend.io/blog/ai-and-privacy, 10.10.2024.
27. Torrance, A.W., Tomlinson, B. (2023). Training Is Everything: Artificial Intelligence, Copyright, and Fair Training. *Dickinson Law Review*, *Vol. 128, Iss. 1*, pp. 233-255, doi: 10.48550/arXiv.2305.03720.
28. Turing, A. (1950). Computing Machinery and Intelligence. *Mind, Vol. LIX, Iss. 236*, pp. 433-460. Retrieved from: https://academic.oup.com/mind/article/LIX/236/433/986238, 10.10.2024.
29. Uzialko, A. (2024). *How Artificial Intelligence Will Transform Businesses*. Retrieved from: https://www.businessnewsdaily.com/9402-artificial-intelligence-business-trends.html, 10.10.2024.

30. Vidal, K. (2024). *Inventorship Guidance for AI-Assisted Inventions. A Notice by the Patent and Trademark Office on 02/13/2024.* Retrieved from: https://www.federalregister.gov/documents/2024/02/13/2024-02623/inventorship-guidance-for-ai-assisted-inventions, 10.10.2024.

31. Yalamati, S. (2023). AI and Risk Management: Predicting Market Volatility. *ESP Journal of Engineering & Technology Advancements, Vol. 1, Iss. 2,* pp. 89-101, doi: 10.56472/25838628/IJACT-V1I2P110

32. Yampolskiy, R.V. (2024). *AI: Unexplainable, Unpredictable, Uncontrollable*. London: Chapman & Hall.