Bialystok Legal Studies
Białostockie Studia Prawnicze
2026 vol. 31 no. 3

DOI: 10.15290/bsp.2026.31.03.01

Received: 21.10.2025
Accepted: 13.05.2026

Daniel Milewski
Warsaw University of Economics, Poland
kontakt@danielmilewski.pl
ORCID ID: 0000–0002–0023–7118

Cezary Małozięć
SWPS University, Poland
cmaloziec@swps.edu.pl
ORCID ID: 0000–0003–3674–280X

Artificial Intelligence as a Challenge for Human Rights, Labour Law and Antitrust Regulations

Abstract: This article examines challenges that artificial intelligence poses to the protection of human rights, including fundamental rights such as privacy, data protection, the right to work, and the prohibition of discrimination. Among the multiple regulatory dimensions affected by AI, three – the protection of fundamental rights, labour law and antitrust law – have been chosen for closer analysis as the areas in which the recently adopted EU regulatory framework (in particular the AI Act and the Platform Work Directive) produces the most immediate and tangible legal consequences. The study highlights the ethical and legal concerns associated with the rapid development and deployment of AI systems, particularly in contexts that affect individuals' lives and freedoms. Special attention is given to the application of AI in the workplace, where automation and algorithmic decision-making may lead to new forms of inequality, job displacement and biased recruitment or performance evaluation processes. The paper explores the intersection between AI and antitrust law, analysing whether AI can be used to facilitate anti-competitive practices. It considers to what extent algorithm-driven pricing mechanisms act autonomously, and to what degree they may be intentionally influenced or optimized to benefit corporate interests. The article concludes by emphasizing the need for a balanced regulatory approach that promotes innovation while ensuring ethical standards, transparency and accountability.

Keywords: artificial intelligence, human rights, labour law, antitrust law

Introduction

Artificial intelligence (AI) represents one of the most significant determinants shaping contemporary socio-economic transformations. The rapid advancement of machine-learning techniques and the ability to process vast amounts of data have led to the increasing integration of AI-based systems across various sectors – from healthcare and transportation to recruitment, the assessment of creditworthiness and business pricing strategies. The benefits resulting from the implementation of AI-driven technologies are indisputable. However, their unreflective or uncontrolled application may give rise to numerous legal and ethical challenges, which should serve as a stimulus for in-depth doctrinal analysis and the development of comprehensive normative frameworks. In particular, AI has the potential to infringe upon fundamental human rights and freedoms, adversely affect employees' working conditions and shape market competition in ways that may raise concerns regarding compliance with legal principles.

The scope of this study has been deliberately narrowed to three areas in which the legal consequences of AI deployment have already crystallized in binding EU and national regulation and in which the risks materialize primarily at the level of individual rights and the competitive structure of the internal market: the protection of fundamental rights, labour law and antitrust law. This choice does not imply that other branches of law remain unaffected. AI also generates serious challenges for intellectual property law (notably as regards authorship of generative outputs and the scope of the text and data-mining exception under Directive (EU) 2019/790, as well as the fundamental right to intellectual property protected under Article 17(2) of the Charter of Fundamental Rights of the European Union (hereinafter: the CFREU)), for administrative law and the functioning of the administrative state (algorithmic decision-making by public authorities, automated risk-scoring in the administration of social benefits and taxes), for civil liability law and for criminal law (deep-fake offences, AI-assisted fraud). These domains, although equally important, require separate doctrinal treatment and have been the subject of growing, dedicated scholarship; their analysis is not feasible within the format of a single article without sacrificing analytical depth.

Given the potential risks associated with the continued uncontrolled development of artificial intelligence, a series of legislative initiatives have been undertaken at the international, European Union and national levels. These efforts culminated in the entry into force on 1 August 2024 of the AI Act (European Parliament & Council of the European Union, 2024c) and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (Council of Europe, 2024). The AI Act, as a pioneering legislative measure on a global scale, has established a unified legal framework for the development and use of AI systems within the European Union, aiming to promote the creation of human-centred and

trustworthy AI while ensuring a high level of protection for health, safety and fundamental rights as enshrined in the CFREU. At the same time – and, one may say, in parallel – the Council of Europe's Framework Convention introduced the first comprehensive international regulation on artificial intelligence, thereby setting a normative standard of global significance.

1. The issue of human rights protection in the age of AI

Within the catalogue of fundamental rights that are particularly sensitive to the influence of artificial intelligence systems, the right to privacy and the protection of personal data occupy a central position. The reason for this is that AI systems employ machine-learning algorithms and frequently operate on large datasets (Big Data), which often include personal data, for the purpose of making predictions or decisions (Gholipour, 2024, p. 94). Examples of such use include facial recognition algorithms designed to identify individuals in crowds or profiling systems that analyse online behaviour to predict preferences (Gültekin-Várkonyi, 2021, p. 5). Such activities may intrude upon an individual's privacy, especially when conducted without their knowledge or consent. Already in the early years of the 21st century, the European Court of Human Rights emphasized the inherent and high risk associated with the collection and storage of sensitive data by governmental entities, noting that individuals have legitimate legal concerns regarding the future use of previously gathered data (Judgments of the ECtHR, 2006 and 2008). Rapid technological advancement has only intensified these concerns.

Another significant threat concerns algorithmic discrimination, which runs counter to the principle of equal treatment. Algorithms trained on historical data may unwittingly perpetuate biases and stereotypes present in the data. The literature contains numerous examples of bias in AI systems, ranging from automated recruitment systems favouring men over women (based on data from male-dominated sectors, or training datasets influenced by patterns such as longer employment interruptions among women due to maternity leave) to credit-scoring algorithms discriminating against certain social classes (Packin & Lev Aretz, 2018, p. 4). Such practices may be deemed violations of the prohibition on discrimination protected by Article 21 of the CFREU, Article 32 of the Constitution of the Republic of Poland ('Equality before the law; Prohibition of discrimination') and Article 113 of the Polish Labour Code ('Prohibition of discrimination in employment'), among others. Importantly, the absence of a direct intent to discriminate is no exemption from liability: if the functioning of an algorithm results in indirect discrimination against certain groups (e.g. through disproportionately frequent rejection of their candidacies in recruitment), an employer or entity applying such an algorithm may face legal consequences under equal treatment provisions.

Freedom of speech and the right to access information constitute another potentially vulnerable area. An increasing amount of content is moderated or filtered through AI, particularly on online platforms and social media. Algorithms can automatically remove specific types of content (such as hate speech) or limit their reach. While this aims to protect users, it also creates the risk of excessive censorship or the misidentification of lawful content as prohibited – so-called false positives (Cobbe, 2021, pp. 741–755). A lack of transparency regarding the criteria used by such algorithms hampers verification of whether freedom of expression (protected under Article 54 of the Constitution of the Republic of Poland and Article 10 of the European Convention on Human Rights) is being infringed. Likewise, algorithms that personalize content for users (recommender systems) may create so-called information bubbles and contribute to opinion polarization, prompting questions about the safeguarding of information pluralism – a foundation of a democratic state.

In the face of the *sui generis* nature of threats arising from the use of AI-based technologies, the European Union possesses an adequate normative apparatus and is not without effective legal safeguards. Consequently, the EU has developed one of the strictest legislative frameworks worldwide in this field: Regulation (EU) 2016/679 of the European Parliament and of the Council (the General Data Protection Regulation, GDPR), applied since 2018, which also indirectly applies to AI systems processing personal data. The GDPR establishes principles such as data minimization, purpose limitation and transparency, along with data subjects' rights (access, rectification, objection, erasure, etc.), collectively forming important protections against abuses in profiling and monitoring individuals through AI (Jędrzejczak, 2024, p. 91).

The second key legal act, which comprehensively regulates uniform legal frameworks for the development and deployment of AI systems within the EU, is the aforementioned AI Act. Its primary objective is to ensure that AI systems placed on the EU market are safe, transparent, non-discriminatory, and subject to human oversight. The Regulation adopts a risk-based approach, establishing categories of AI systems with varying degrees of risk to users and society, along with corresponding restrictions. Thus systems posing an unacceptable risk to EU values have been qualified as prohibited AI practices, while high-risk AI systems are subject to stringent requirements before market entry. Prohibited AI practices under the AI Act include:

a) systems leading to cognitive manipulation of humans (e.g. interactive toys or applications inducing children to engage in dangerous behaviours) (Article 5(1)(a)),
b) systems exploiting vulnerabilities based on age, disability or social or economic status, causing changes in people's behaviour in a way likely to cause significant harm (Article 5(1)(b)),
c) social scoring, i.e. a comprehensive evaluation of citizens based on their behaviour or attributes when results lead to unfair treatment in unrelated

social contexts, or unjustified or disproportionate harm to individuals or groups (Article 5(1)(c)),

d) AI systems for assessing or predicting the risk of a person committing a rime based solely on profiling or evaluation of personality traits. This prohibition will not apply to AI systems that support human assessment of a person's involvement in criminal activity when that assessment is based on objective and verifiable facts directly related to criminal conduct (Article 5(1)(d)),
e) AI systems that create or expand facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage (Article 5(1)(e)),
f) use of emotion recognition technology in workplaces and educational institutions (Article 5(1)(f)),
g) biometric categorization systems that categorize individual natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation (Article 5(1)(g)),
h) real-time biometric identification of individuals in public spaces (Article 5(1)(h)).

These categories have been deemed so dangerous to fundamental human rights (particularly privacy, human dignity and individual freedom) that the EU legislature has established a general ban on their use within the European Union. Only in certain exceptional cases may they be authorized (e.g. real-time facial recognition by police strictly for locating perpetrators of the most serious crimes, subject to judicial authority or an independent administrative authority). As a rule, however, the EU establishes a clear boundary to protect democratic values.

High-risk AI systems are those which, despite potential threats to safety and human rights, also offer significant benefits to individuals. Accordingly, the AI Act permits them on the market solely upon their meeting additional conditions. Annex III enumerates critical sectors, including:

a) critical infrastructure (e.g. systems managing critical digital infrastructure, road traffic),
b) education and vocational training (e.g. AI systems used for admission decisions in educational institutions, for evaluating learning outcomes, assessing what level of education or training a person should receive or can access, monitoring or detecting prohibited behaviour by students during exams),
c) essential private and public services (e.g. credit-scoring systems, systems used by or for public authorities to assess eligibility for public ben-

efits or services, systems used for risk assessment and pricing for health insurance),
d) the judiciary (e.g. systems assisting courts in analysing facts and interpreting legal provisions, systems supporting criminal investigations),
e) border control (e.g. identification systems in migration and border procedures),
f) biometrics, insofar as their use is permitted under relevant Union or national law: remote biometric identification systems or emotion recognition, used for biometric categorization based on protected attributes,
g) employment, worker management and access to self-employment (for the requirement used to make decisions about employment conditions, promotion, termination, task allocation),
h) law enforcement (e.g. systems used to assess a person's risk of becoming a crime victim or of someone offending or reoffending, not based solely on profiling or personality traits, polygraphs or lie-detectors, as well as systems used to evaluate the reliability of evidence during criminal investigations or prosecutions).

Providers and users of high-risk AI systems must meet multiple obligations to ensure respect for rights and safety. These include implementing risk-management systems (Article 9 AI Act), ensuring high-quality training data to minimize errors and biases (Article 10), maintaining documentation and incident records for audit purposes (Article 12), informing users about AI features and limitations (Article 13), introducing appropriate mechanisms for human oversight (Article 14), and complying with cybersecurity and performance accuracy standards (Article 15). Of particular note is the requirement imposed on public-sector or private entities providing public services to conduct a Fundamental Rights Impact Assessment, identifying which specific rights or freedoms may be affected by the AI system and what measures should be taken to mitigate such risks. This obligation underscores the overarching goal of regulation: preventing human rights violations before they occur, through a systematic and preventive analysis of the impact of AI applications on fundamental rights, intended to secure accountability, transparency and the ethical development and use of AI systems (Bertaina et al., 2025, p. 2).

In addition to the EU measures, it is worth noting the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS no. 225), adopted by the Committee of Ministers on 17 May 2024 and opened for signature in Vilnius on 5 September 2024. The two instruments – the AI Act and the Framework Convention – although complementary, differ fundamentally in their legal nature and operative effect. The AI Act is an EU regulation directly applicable in all Member States, harmonizing rules for the placing on the market and use of AI systems, prescribing concrete obligations addressed to providers, deployers,

importers and distributors, and equipped with a centralized enforcement architecture (the AI Office, national competent authorities and administrative fines that for the most serious infringements reach EUR 35 million or 7% of global annual turnover). The Framework Convention, by contrast, is a public international law treaty of a framework character, addressed to state parties; it sets out general principles and obligations of result rather than detailed rules of conduct, leaves parties broad discretion as to the means of compliance (Article 3(1)(b) allows alternative measures vis-à-vis the private sector), excludes matters of national defence (Article 3(2)) and lacks an autonomous sanctioning mechanism, relying instead on a Conference of the Parties as a follow-up body. As of the date of writing, the Framework Convention has not yet entered into force: entry into force is conditional upon five ratifications, including by at least three Council of Europe Member States (Article 30(2)). The European Union signed the Convention on 5 September 2024 on the basis of Council Decision (EU) 2024/2218; for the EU the Convention is to be implemented, in the area of its exclusive competence, through the AI Act itself. The Framework Convention thus complements but does not replace the EU regime: it contributes to building a global baseline (the United Kingdom as a Council of Europe member, and the United States and Israel as non-member states involved in its elaboration, signed it on the same day; other non-Council-of-Europe states may accede under Article 31), while the substantive density of legal protection within the single market is determined by EU law (Presno Linera & Meuwese, 2024, p. 148).

At the national level, in Poland, protection against potential human rights abuses involving AI is largely based on implementing the aforementioned international and EU frameworks. The Constitution of the Republic of Poland guarantees fundamental rights (such as dignity, privacy, freedom of speech and equality) regardless of the nature of the threat, implying that actions involving algorithms must also comply with constitutional limits (Kaczmarek-Templin, 2024, p. 27). It is worth noting that the catalogue of fundamental rights affected by AI is broader than the analysis above suggests; it extends in particular to the right to intellectual property under Article 17(2) of the CFREU (and, correspondingly, Article 1 of Protocol no. 1 to the European Convention on Human Rights as interpreted by the Strasbourg Court). The intellectual-property dimension, however, situates itself primarily on the positive side of the protection – the entitlements of authors and right-holders vis-à-vis AI systems – whereas the analytical axis pursued in this article concerns the negative side, namely the protection of fundamental rights against infringements by AI systems. The two perspectives are complementary but methodologically distinct, and the former forms the subject of a separate strand of scholarship.

Given this comprehensive, multi-level set of legal instruments, from general constitutional and international norms to the GDPR and AI Act, the normative safeguard framework appears to provide adequate and high-quality legal protection. The remaining challenge lies in supervisory bodies (e.g. the president of the Personal

Data Protection Office in Poland in the area of data protection, or the future European AI Office established under the AI Act) effectively implementing these norms in practice and ensuring awareness among entities developing and deploying AI regarding their obligations.

2. AI, protection of employees' rights, and the future of employment: Automation, supervision and HR decisions

The labour market has also been significantly affected by the widespread implementation of AI systems, which are increasingly shaping not only the organization of work but also the nature of the employment relationship and the position of the employee in relation to the employer. Several key aspects of AI's impact on employment can be identified. The first is the automation of work through the replacement of people by intelligent machines or algorithms to perform certain tasks. Gradually, more and more factories are equipping their production lines with intelligent robots that use AI to take over repetitive tasks. Call centres employ artificial intelligence algorithms for customer service (chatbots, voicebots); intelligent avatars teach the basics of foreign languages; and software can rapidly analyse large sets of financial data and draw conclusions. On the one hand, technological progress significantly increases labour productivity that previously required the involvement of numerous assistants and analysts. On the other hand, it raises concerns about job security and the growth of so-called technological unemployment (Tyson & Zysman, 2022, p. 259). Economic studies indicate that algorithmic progress may particularly endanger medium-skilled occupations performing routine tasks, but increasingly also intellectual professions, as AI develops the ability to process natural language and make quasi-expert decisions (Drydakis, 2025).

Labour law provisions do not protect against job elimination for technological reasons – employers are entitled to reorganize their workplaces and introduce new technologies, even if this results in redundancies (with due respect for notice and collective dismissal regulations). Nevertheless, it is increasingly postulated that legislative policy should accompany the processes of AI-driven job replacement by introducing measures to mitigate social impacts. One such measure is strengthening employees' right to retraining and upskilling, so that those threatened by AI-induced job loss can be reskilled into roles complementary to new technologies (Tyson & Zysman, 2022, p. 266). The European Union has promoted the concept of a 'just transition' in the context of digitalization and automation, reflected in the European Pillar of Social Rights, which endorses lifelong learning and active employment support (Aragüez Valenzuela, 2024, pp. 158–159). In Poland, there are currently no specific legal regulations in this regard; providing suitable training to employees depends largely on employers' willingness or labour-market support programmes. However,

in light of AI's progress, this issue may call for legislative intervention, such as incentives encouraging companies to retrain or upskill rather than dismiss employees.

The second aspect concerns employer supervision of employees using AI, known as 'algorithmic management'. An increasing number of employers use digital systems to monitor working time, productivity or even employee behaviour, and continuous electronic surveillance can infringe upon an employee's dignity and privacy. Polish legislation, under Articles 222 and 223 of the Labour Code, attempts to balance the employer's interests (in protecting property or production control) with employees' rights – requiring, among other things, that employees be informed about the purpose and scope of monitoring, and prohibiting surveillance of sanitary facilities or private correspondence. However, AI opens new possibilities for supervision that go beyond traditional cameras or email monitoring. Programs analysing mouse and keyboard movements (to measure actual working time) or monitoring visual activity are becoming increasingly sophisticated. Some companies have even experimented with cameras analysing employees' facial expressions to assess their concentration or emotional state. In response to such trends, labour laws across Europe are beginning to introduce additional employee protections. For instance, in France and Germany, works councils have statutory rights to co-decide on the introduction of new workplace monitoring technologies; employers cannot implement AI-based surveillance systems without employee representatives' consent. Italy amended its Employees' Statute a few years ago to extend union consent requirements to remote digital monitoring systems (Aloisi & Gramano, 2019, pp. 116–123).

The third area concerns AI-assisted HR decision-making, including recruitment, employee evaluation, promotion and dismlissal. In recruitment, AI most often takes the form of applicant tracking systems, which automatically analyse submitted CVs and reject those that do not meet pre-defined criteria, selecting a handful of candidates from hundreds for interviews with HR staff. Algorithmic CV filtering, however, may lead to the use of opaque selection criteria, leaving candidates unaware of the reasons for their rejection. Such operations can result in indirect discrimination risks if, for example, a system trained on the profiles of existing employees favours a certain group (e.g. graduates from specific universities) over others (Rigotti & Fosch-Villaronga, 2024, p. 5).

From a labour law perspective, recruitment decisions, although subject to employers' discretion, are constrained by anti-discrimination provisions. A job applicant subjected to unequal treatment based on a protected attribute (sex, age, origin, disability, etc.) may claim compensation under Article 183(d) of the Labour Code. If discriminatory grounds for refusal are proven, the employer bears liability, irrespective of whether the selection was carried out by a human or an algorithm. Therefore employers implementing AI in recruitment should examine their algorithms for bias and ensure the possibility of human verification in atypical cases to avoid such claims (Rigotti & Fosch-Villaronga, 2024, p. 6). In fact, employers using AI systems to se-

lect candidates for employment should also verify whether their AI software supplier meets all the requirements of a high-risk system category (Articles 8–21 AI Act). If the AI system is categorized as high-risk, deployers who are employers must inform employees' representatives about use of the system before using it in the workplace (Article 26(7) AI Act). Data protection must not be overlooked either: since candidates' personal data are processed during recruitment, under the GDPR they have the right to be informed if a decision rejecting their application was made automatically and to object or request human review (Article 22 GDPR).

Analysis of the above issues demonstrates that the integration of AI systems can infringe or weaken employee rights such as the right to dignity and privacy, the right to equal treatment or the right to be informed of evaluation criteria. Nonetheless, protecting these rights requires the proper interpretation of existing provisions and, where necessary, the introduction of new regulations adapted to the algorithmic era. Recognizing this, the European Union has identified the need to regulate the influence of digital platforms and algorithms on working conditions. This initiative was reflected in the adoption of the Platform Work Directive on 23 October 2024 (European Parliament & Council of the European Union, 2024a), which aims to regulate and improve working conditions for persons providing services through online platforms. Moreover, it introduces the concept of algorithmic management into European law, along with associated employee rights, which may also extend beyond the platform sector. EU Member States have until 2 December 2026 to align their national legislation with these new EU requirements.

Crucially, with respect to algorithmic management, the Directive obliges employers using automated monitoring and decision-making to ensure algorithmic transparency and human oversight over systems making significant HR decisions (which is also consistent with the AI Act provisions regulating high-risk systems). Practically, this entails obligations such as informing employees about the use of automatic monitoring and performance-evaluation systems, clearly explaining in understandable terms the criteria and parameters applied, and providing employees with the possibility to contact competent personnel for reviews of algorithm decisions (Articles 7–15 Platform Work Directive). Similar obligations are also imposed under the AI Act (Article 26(7)).

Taking into account both EU law (the Platform Work Directive and the AI Act provisions on high-risk systems linked to HR processes) and national-level developments (Labour Code amendments in some countries and future implementation of the Directive in Poland), these efforts aim to close regulatory gaps and ensure that employees' fundamental rights – from privacy to fair treatment – are equally respected in modern and automated work environments.

3. AI as a challenge for antitrust regulations

Advanced AI systems are gradually playing an increasingly significant role in the functioning of markets and in shaping companies' business strategies. This inevitably affects the field of competition policy. The primary objective of antitrust law (referred to as competition law in Europe) is to ensure fair market rivalry, notably through the prohibition of anti-competitive agreements such as price-fixing, market sharing or production-limiting cartels (Article 102 TFEU; Articles 6 and 9 of the Act on Competition and Consumer Protection) (Rab, 2019, p. 141).

The emergence of AI and advanced algorithms raises the question of whether traditional anti-competitive practices may evolve into newer, more effective forms through technological means, and whether the existing legal framework can detect and penalize such phenomena. Traditionally, in order for a competition authority to find the existence of a price-fixing cartel between specific entities, it must demonstrate that an agreement or a concerted practice exists between independent undertakings, typically in the form of secret meetings or communication. AI technology, however, may expand the range of circumstances considered prohibited practices under competition and consumer protection law. One of the most frequently discussed risks is the rise of algorithmic price-fixing (Rab, 2019, pp. 141–143). In the digital economy, companies selling goods and services to consumers, as well as online platforms, increasingly rely on dynamic-pricing algorithms that continuously monitor competitors' prices and adjust their own accordingly. Problems may arise when several firms use algorithms developed by the same software provider, thereby unintentionally facilitating price harmonization on the market without any formal interaction among company executives.

An illustrative scenario of such tacit algorithmic collusion would involve several petrol station owners delegating pricing decisions to algorithms. These algorithms then analyse each other's pricing behaviours and may 'reach a shared understanding' whereby all maintain fuel prices above the cost-optimal level, effectively forming a cartel without human decision-makers' involvement. This phenomenon could enable corporations to circumvent antitrust laws. Consequently, there is concern that companies may use algorithms as a form of 'hidden collusion': legally, they do not engage in any agreement, yet their algorithms stabilize prices at an elevated level (Mleczko, 2018, p. 70).

Since Article 6 of the Act on Competition and Consumer Protection of 16 February 2007 prohibits agreements that have as their object or effect the restriction of competition (including price coordination), it might initially seem that in the absence of direct human contact, there can be no 'agreement' to speak of. Yet competition law doctrine recognizes the concept of a 'concerted practice': conscious coordination between undertakings, even without a formal contract, may suffice to render their conduct potentially anti-competitive (Jurkowska-Gomułka & Piszcz, 2025, pp. 225–226).

Therefore if it can be demonstrated that companies intentionally used algorithms in a manner that enabled them to anticipate and adjust prices more effectively, an antitrust authority may attempt to attribute a violation of competition law to them and consequently impose a financial penalty. Establishing awareness and intent will be crucial – for instance, proving that firms knew of concurrent use of the same algorithm or adjusted its parameters to avoid price wars. In such cases, the algorithm remains merely a tool, and responsibility lies with the undertakings themselves.

Legal literature underscores that sanctions cannot be avoided simply because a decision was made by an algorithm if that algorithm acted under human-defined instructions aimed at restricting competition. Importantly, the liability of the undertaking for AI actions in the field of competition and consumer protection law should be the rule, since allowing an exemption based on the algorithm's autonomy would pose too great a risk of abuse. In other words, a company cannot justify itself by claiming 'it wasn't us who fixed the prices; our algorithms decided that'; once a firm deploys pricing algorithms, it must supervise their functioning and bear responsibility for their actions, under the principle of strict liability (Stucke & Ezrachi, 2018, pp. 643–644).

This debate is by no means confined to European scholarship. Crane (2024, pp. 1187–1192) argues in the context of US antitrust law that the 'coming wave' of general-purpose AI technologies will erode the foundational assumptions on which competition law has rested: AI-driven systems will detect (and even program) consumer preferences without the benefit of price signals, will invert the salient characteristics of human managerial intent (whose objectives become discernible while operative steps remain opaque) and will enable extreme market concentration that may eventually require sector-specific regulation rather than *ex post* antitrust enforcement. From a European perspective, this diagnosis reinforces rather than displaces the traditional doctrinal toolbox of Article 101 and 102 TFEU and their national counterparts (Article 6 and 9 of the Polish Act on Competition and Consumer Protection), but it counsels integrating the AI Act's transparency, logging and human-oversight obligations (Articles 12, 14 and 26) into the evidentiary architecture of competition proceedings, and complementing them with the *ex ante* asymmetric duties imposed on gatekeepers under Regulation (EU) 2022/1925 (the Digital Markets Act (DMA)). The convergence of these three regulatory layers – traditional antitrust, the AI Act and the DMA – is in our view, the genuinely novel feature of the European response, and it is on the interaction between them that future scholarship and enforcement practice will have to focus.

Conclusions

One of the main concerns associated with artificial intelligence is the ethical dimension of its use and the need to ensure that its development respects fundamental human rights. The law often struggles to keep pace with the rapid advancement of

technology; however, the AI Act and the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law provide a solid foundation for safeguarding fundamental rights and ensuring the safe and responsible deployment of AI technologies. The rapid evolution of such systems may nevertheless lead to violations of the right to privacy and data protection. The extraordinary capacity of AI to process information, correlate facts and analyse materials from the internet or surveillance systems raises legitimate fears of an Orwellian vision of a permanently monitored society being realized.

Equally important are the risks associated with algorithmic discrimination, which may result from biased data, prejudice or flaws in the machine-learning process. Poorly designed AI systems can cause tangible harm, restricting access to education, employment or public benefits, or even endangering life and health when used in medical contexts. The key challenge therefore lies in ensuring that AI systems are fair, transparent and pluralistic. The AI Act rightly classifies systems related to recruitment, employment and access to education as high-risk, which should be positively assessed given their significant impact on individuals' livelihoods, career prospects, economic well-being and labour rights. Nonetheless, there is a legitimate concern that the automation of decision-making processes may lead to new forms of inequality, social exclusion and even rising unemployment.

The development of advanced AI systems also raises challenges in the field of competition law, particularly regarding the detection and prevention of collusive behaviour. Algorithms used for dynamic pricing may result in unintended price harmonization among enterprises, even in the absence of formal agreements. In such cases, competition authorities may qualify the conduct of undertakings as a form of concerted practice, especially where there is evidence of awareness or the intentional use of algorithms to limit competition.

The decisive question is how the balance postulated above is to be achieved in practice and how the policy goals of the EU regulatory framework are to be translated from the level of legislative declaration to the level of operational reality. In our view, three interlocking elements are indispensable. First, the institutional architecture: Article 70 of the AI Act requires Member States to designate a national market surveillance authority for AI Act enforcement. The Polish draft Act on Artificial Intelligence Systems (parliamentary print no. 2443) opts for a dedicated regulator: Article 5(1) of the draft establishes the Commission for the Development and Safety of Artificial Intelligence (Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji) as the market surveillance authority within the meaning of Article 70(1) of the AI Act, and Article 5(2) designates the Commission as the single point of contact within the meaning of Article 70(2). The choice of a dedicated regulator concentrates technical expertise but also creates a risk of jurisdictional fragmentation in cases that simultaneously implicate data protection, competition or labour law dimensions; its effectiveness will depend on the quality of cooperation arrangements with sectoral

regulators and on the genuine resourcing of the Commission with technical, and not only legal, expertise.

Second, the architecture of judicial review: under the new Article 479(88)(a) of the Code of Civil Procedure, introduced by the draft Act, appeals against decisions of the Commission fall to the Court of Competition and Consumer Protection (Sąd Ochrony Konkurencji i Konsumentów). This choice consciously assimilates judicial control of AI Act enforcement to the established model of cases in the regulated sector (competition, energy, electronic communications, rail transport), ensuring consistency of procedural standards.

Third, private law remedies: following the withdrawal of the proposed AI Liability Directive in February 2025, the civil liability framework for AI-related harm rests on the EU side on the revised Product Liability Directive (Directive (EU) 2024/2853) and on the Polish side on the general regimes of tort and contractual liability under the Civil Code, applied by analogy to AI systems. Article 415 of the Civil Code, which establishes the general clause of fault-based tort liability, allows the injured party to seek redress against the operator or deployer of an AI system whose unlawful and culpable conduct – including failure to exercise due supervision over an autonomously acting system – has caused damage. Where the harm arises in the performance of a contractual obligation, Article 471 of the Civil Code grounds the liability of the debtor for non-performance or improper performance of an obligation, regardless of whether the breach was the immediate result of a human decision or of the operation of an AI system used by the debtor in the discharge of the obligation. The Product Liability Directive reform complements these regimes by extending the notion of 'product' to software, including AI systems, and by introducing presumptions of defect and causation in technically complex cases – changes which, properly implemented in Polish law, may compensate for the absence of a dedicated AI-liability instrument.

A methodological caveat is in order. The ultimate test of the AI Act will not be the consistency of its wording but the capacity of national authorities and courts to enforce its norms under conditions of informational and technological asymmetry between regulator and regulated. This observation corresponds, *mutatis mutandis*, to Crane's account, formulated for the United States antitrust order, of an emerging 'AI arms race between firms and enforcers' in which, on present trajectories, 'the firms have the decided advantage' (2024, p. 1224; see also pp. 1225–1226 on the difficulty of cartel detection in algorithmic environments). The European answer to this asymmetry differs from the solution envisaged by Crane: it does not consist in a retreat from antitrust toward purely sector-specific regulation but in the layering of three regimes – *ex post* competition enforcement, *ex ante* regulation of gatekeepers under the DMA, and horizontal AI regulation under the AI Act. The Polish model – a specialized Commission, a distinct procedural regime, a dedicated complaint mechanism and the assimilation of judicial review to the established model of regulated-sector cases

– is a coherent national translation of that European regulatory wager. The thesis defended in this article is, accordingly, that the convergence of the three mechanisms outlined above – institutional, judicial review, and private law – is what may transform the European regulatory model from a normative aspiration into a functioning system of protection. None of these mechanisms considered in isolation will be sufficient; only their coordinated application can keep technological innovation within the bounds of fundamental rights, fair competition and democratic accountability.

REFERENCES

Aloisi, A., & Gramano, E. (2019). Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context. *Comparative Labor Law & Policy Journal*, *41*(1), 101–138.

Aragüez Valenzuela, L. (2024). Hacia la transición justa y sostenible del empleo digitalizado. Algunas reflexiones sobre la formación profesional y el Plan Europeo de Acción de Educación Digital. (2021–2027). *E-Revista Internacional de la Protección Social*, *9*(2), 157–179.

Bertaina, S., Biganzoli, I., Desiante, R., Fontanella, D., Inverardi, N., Penco, I. G., & Cosentini, A. C. (2025). Fundamental rights and artificial intelligence impact assessment: A new quantitative methodology in the upcoming era of AI Act. *Computer Law & Security Review, 56*, Article 106101. https://doi.org/10.1016/j.clsr.2024.106101

Cobbe, J. (2021). Algorithmic censorship by social platforms: Power and resistance. *Philosophy & Technology*, *34*, 739–766.

Council of Europe. (1950). European Convention on Human Rights, signed in Rome on 4 November 1950 (Dz.U. 1993 no. 61, pos. 284).

Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, Vilnius, 5 September 2024 (CETS no. 225).

Council of the European Union. (2024). Council Decision (EU) 2024/2218 of 28 August 2024 on the Signing, on Behalf of the European Union, of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (O. J. L, 06.09.2024).

Crane, D. A. (2024). Antitrust after the coming wave. *New York University Law Review*, *99*(4), 1187–1243.

Drydakis, N. (2025). Artificial intelligence and labor market outcomes. *IZA World of Labor, Article 514. https://doi.org/10.15185/izawol.514*

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

European Parliament & Council of the European Union. (2019). Directive (EU) 2019/790 of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC (DSM Directive) (O. J. L 130, 17.05.2019, 92–125).

European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/1925 of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (O. J. L 265, 12.10.2022, 1–66).

European Parliament & Council of the European Union. (2024a). Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on Improving Working Conditions in Platform Work (O. J. L 2024/2831, 11.11.2024).

European Parliament & Council of the European Union. (2024b). Directive (EU) 2024/2853 of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC (O. J. L 2024/2853, 18.11.2024).

European Parliament & Council of the European Union. (2024c). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No. 300/2008 (EU) No. 167/2013 (EU) No. 168/2013 (EU) No. 2018/858 (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (O. J. L 2024/1689, 12.07.2024).

European Union. (1957). Treaty on the Functioning of the European Union, signed in Rome on 25 March 1957. (Dz.U. 2004 no. 90, pos. 864).

European Union. (2012). Charter of Fundamental Rights of the European Union (consolidated version: O. J. C 326, 26.10.2012).

Gholipour, M. (2024). The impact of machine learning algorithms and big data on privacy in data collection and analysis. *Australian Journal of Engineering and Innovative Technology*, *6*(5), 93–103.

Gültekin-Várkonyi, G. (2021). Facial recognition technologies and human rights: A European law perspective. *Hungarian Journal of Legal Studies*, *62*(4), 392–408.

Jędrzejczak, M. (2024). Ochrona danych osobowych przetwarzanych przez systemy sztucznej inteligencji. *Gdańskie Studia Prawnicze*, *3*(64), 86–98.

Judgment of the European Court of Human Rights of 7 December 2006 on the case of *Van der Velden v. the Netherlands*, application no. 29514/05.

Judgment of the European Court of Human Rights of 4 December 2008 on the case of *S. and Marper v. the United Kingdom*, application nos. 30562/04 and 30566/04.

Jurkowska-Gomułka, A., & Piszcz, A. (2025). Komentarz do artykułu 6. In A. Jurkowska-Gomułka & A. Piszcz (Eds.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz* (pp. 225–226). C. H. Beck.

Kaczmarek-Templin, B. (2024). Justice in the machine age: Legal landscapes and challenges in the disputes in the era of artificial intelligence – remarks in the light of Polish regulations. In *Artificial intelligence and legal responsibility* (pp. 19–28). Iberojur Science Press. https://doi.org/10.62140/BKT192024

Mleczko, M. (2018). Technologiczne wyzwania dla antropocentrycznego prawa konkurencji na przykładzie algorytmicznego ustalania cen w sektorze e-commerce. *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, *8*(7), 63–72.

Packin, N. G., & Lev-Aretz, Y. (2018). Learning algorithms and discrimination. In W. Barfield & U. Pagallo (Eds.), *Research handbook on the law of artificial intelligence* (pp. 88–113). Edward Elgar. https://doi.org/10.4337/9781786439055.00014

Presno Linera, M. Á., & Meuwese, A. (2024). La regulación de la inteligencia artificial en Europa. *Teoría y Realidad Constitucional*, *54*, 131–161.

Rab, S. (2019). Artificial intelligence, algorithms and antitrust. *Competition Law Journal*, *18*(4), 141–150.

Rigotti, C., & Fosch-Villaronga, E. (2024). *Fairness, AI & recruitment. Computer Law & Security Review, 53*, Article 105966. https://doi.org/10.1016/j.clsr.2024.105966

Sejm of the Republic of Poland. (1964). Act of 23 April 1964 – Civil Code (consolidated text: Dz.U. 2024, item 1061, as amended).

Sejm of the Republic of Poland. (1974). Act of 26 June 1974 –Labour Code (consolidated text: Dz.U. 2025, item 277).

Sejm of the Republic of Poland. (2007). Act of 16 February 2007 on Competition and Consumer Protection (consolidated text: Dz.U. 2024, item 1616).

Stucke, M. E., & Ezrachi, A. (2018). Antitrust, algorithmic pricing and tacit collusion. In W. Barfield & U. Pagallo (Eds.), *Research handbook on the law of artificial intelligence* (pp. 624–640). Edward Elgar.

Tyson, L. D., & Zysman, J. (2022). Automation, AI & work. *Daedalus*, *151*(2), 256–271.