Volume 10 ▪ Autumn 2025 ▪ Number 4

KAZAN UNIVERSITY LAW REVIEW

TABLE OF CONTENTS

ARTICLES

CONFERENCE REVIEWS

• ПРОСПЕКТ •

KAZAN UNIVERSITY LAW REVIEW

Volume 10, Autumn 2025, Number 4

kazanlawreview.org

KAZAN UNIVERSITY LAW REVIEW

Volume 10, Autumn 2025, Number 4

kazanlawreview.org

«KAZAN UNIVERSITY LAW REVIEW»
(registered by The Federal Service
for Supervision of Communications,
Information Technology
and Mass Communications
on 17 November 2016
(certificate number PI № FS 77-67763
(ПИ № ФС 77-67763))

Editorial office:
room 326, 18 Kremlyovskaya St.,
Kazan, 420008 Russia, Republic of Tatarstan

Publishing office:
Building 4, 7, Borovaya St.,
Moscow, 111020, Russia

Founders of the mass media:
Federal State Autonomous Educational Institution of Higher Education "Kazan (Volga region) Federal University"; "Publishing house "STATUT" Ltd.; "Yurlit" Ltd.

ISSN 2541-8823 (print)
ISSN 2686-7885 (online)

Publication:
four issues per year (one issue per quarter)

The reprint of materials of the journal "Kazan University Law Review" is allowed only with the consent of the Publisher. Link to the source publication is obligatory. The Publisher or the Editor's office does not render information and consultations and does not enter into correspondence. Manuscripts can not be returned. The Founder and the Publisher are not responsible for the content of advertisements and announcements.

Opinions expressed in the contributions are those of the authors and do not necessarily reflect the official view of the organizations they are affiliated with or this publication. The journal is indexed/abstracted in ERIH PLUS, HeinOnline, eLIBRARY.RU

Dear readers,

It is my pleasure to present to you the fourth regular issue of the journal “Kazan University Law Review” in 2025.

This issue is dedicated to exploring the profound and complex transformations occurring within modern legal systems under the influence of technological innovation and global challenges. The articles presented herein critically examine how artificial intelligence, digital management, and international cooperation are reshaping the foundations of criminal justice, labour relations, and human rights protection.

The issue opens with the comprehensive study “AI in criminal justice: a comparative study of predictive policing, risk assessment, and sentencing algorithms” of Sohel Rana. This paper provides a rigorous cross-jurisdictional analysis of algorithmic tools in the criminal justice systems of the United States, the United Kingdom, and China. By scrutinizing systems like COMPAS and PredPol, the authors illuminate the pervasive ethical and legal dilemmas of algorithmic bias, transparency deficits, and threats to due process. The study concludes with vital, context-sensitive policy recommendations, offering a crucial framework for nations like Bangladesh that are navigating the initial stages of AI integration into their legal infrastructure.

The discussion then turns to the evolving landscape of labour law with the article by I.A. Filipova and I.R. Begishev, titled “Protection of employees’ personal data in the context of the spread of algorithmic management (based on court practice)”. The authors provide a timely examination of how the rise of algorithmic management and AI-driven workplace surveillance intensifies risks to employee privacy and data security. Grounding their analysis in a review of emerging Russian court practice, they identify significant gaps in current legal frameworks. The article persuasively argues for the urgent need to update labour legislation, including reinstating a robust legal definition of employee personal data, to safeguard fundamental rights in the digitally transforming workplace.

The “Conference Reviews” section features a report on the outcomes of the 10th International Scientific and Practical Convention of Students and Postgraduates “Vector of Law: Global Challenges and the National Code”. Held at Kazan Federal University, this event served as a dynamic platform uniting over 250 students and young scholars from across Russia and neighbouring countries. The review highlights the convention’s role in fostering professional dialogue, honing practical legal skills through moot courts, and engaging the next generation of lawyers with the pressing legal questions of our time.

Together, these contributions underscore a central theme of contemporary jurisprudence: the imperative to balance technological advancement and efficiency with the unwavering protection of human rights, fairness, and the rule of law. This issue aims to contribute meaningfully to the global scholarly dialogue on navigating this critical balance.

With best regards,
Editor-in-Chief
Damir Valeev

TABLE OF CONTENTS

ARTICLES

CONFERENCE REVIEWS

ARTICLES

Sohel Rana

Candidate of Legal Sciences (PhD in Criminal Law, University of Malaya, Malaysia), Assistant Professor, Department of Law, University of Information Technology and Sciences (UITS)

AI IN CRIMINAL JUSTICE: A COMPARATIVE STUDY OF PREDICTIVE POLICING, RISK ASSESSMENT, AND SENTENCING ALGORITHMS

DOI: 10.30729/2541-8823-2025-10-4-164-189

Abstract. *This article provides a thorough analysis of the use of artificial intelligence (AI) in criminal justice systems, with a particular emphasis on predictive policing, risk assessment approaches, and sentencing algorithms. The analysis weighs the implications of algorithmic decision-making in relation to issues of fairness, transparency, due process, and underlying prejudices by comparing the COMPAS system in the United States, the PredPol system in the United Kingdom, and AI-based policing technologies in China. Methodologically, this study employs doctrinal and comparative legal approaches, supplemented by inter-disciplinary ideas from technology and ethics. The findings highlight widespread challenges across jurisdictions, including racial discrimination, socioeconomic bias, a lack of transparency, and insufficient supervision measures. Furthermore, the research analyses the perceived potential and hazards of using these technologies in Bangladesh's expanding legal infrastructure. Finally, the article recommends for the institutionalisation of regulatory measures, oversight bodies, and context-based adjustments that are essential to guarantee that the use of AI in criminal justice adheres to the principles of justice, human rights, and democratic accountability.*

Keywords: *Algorithmic bias, Automated decision-making, Due process, Legal accountability, Risk assessment tools.*

1. Introduction

The art of artificial intelligence (AI) is rapidly transforming multiple sectors, with a particular emphasis on the criminal justice sector, where related technologies are increasingly used to advance or perfect decision-making processes related to crime prediction, risk assessment, and sentence. Such systems use complicated algorithms to analyse large databases, discover trends, and generate predictive analysis, which can increase efficiency, accuracy, and evidence-based decision-making in the criminal justice system[1]. Such innovation mirrors broader technical and cultural shifts that challenge existing legal frameworks, raising serious concerns about technology's ability to enhance justice, fairness, and human rights safeguards.

Predictive policing, risk assessment tools, and sentencing algorithms are some of the most common AI uses in criminal justice. Predictive policing systems use previous crime data and social variables to anticipate prospective crime hotspots or repeat offenders, allowing law enforcement to spend resources more efficiently. Risk assessment algorithms calculate the chance of criminals reoffending or failing to appear in court, impacting choices on bail, parole, or punishment harshness. Sentencing algorithms let judges make data-driven decisions based on previous case results and risk factors. Together, these technologies have the ability to eliminate human error and prejudice, enhance standardised decision-making, and speed up judicial procedures[2].

The implementation of artificial intelligence in the criminal justice system raises fundamental ethical, legal, and societal concerns. These include questions about prejudice, equity, transparency, due process, and accountability. AI algorithms' machine learning methods, which rely on historical data that may reflect current societal biases, frequently reinforce or amplify discrimination against vulnerable demographic groups, particularly ethnic minorities, economically disadvantaged communities, and other high-risk populations[3]. Furthermore, the lack of transparency associated with the vast majority of AI models, known as the "black box", obscures defendants' and their counsel's grasp and capacity to evaluate or question the outcomes generated by these algorithms. Furthermore, the transfer of key adjudicative functions to computer systems raises critical concerns about the preservation of human judgement and the essential concepts of legal responsibility[4].

[1] *Joh E. E.* (2020). Artificial intelligence and policing: First questions // Annual Review of Law and Social Science, 16. Pp. 359–377. https://doi.org/10.1146/annurev-lawsocsci-101518-042816.

[2] *Barabas C., Dinakar K., Ito J., et al.* (2020). Interventions over predictions: How to use AI to help humans make better decisions // Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society.

[3] *Mayson S.* (2021). Bias in, bias out: Algorithmic fairness and the limits of policy // Yale Law Journal, 130(8). Pp. 2140–2210. https://doi.org/10.2139/ssrn.3478377.

[4] *Burrell J., Knox H., Obrock M.* (2021). Transparency and oversight of risk assessment tools in criminal justice // Criminal Justice Ethics, 40(1). Pp. 3–21. https://doi.org/10.1080/0731129X.2020.1812149.

In this context, a comparative study of the application of artificial intelligence in the criminal justice system is essential to understanding how various jurisdictions approach and employ these technologies. This study examines three significant cases: COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) in the United States, PredPol (Predictive police) in the United Kingdom, and AI-powered police systems in China.

COMPAS is frequently used in the United States to assess pretrial risk and recommend sentences, although it has been criticism for concerns of racial prejudice and transparency[1]. PredPol, which was developed in the United States before being used in the United Kingdom, combines geographical and temporal data to anticipate crime hotspots; however, its effectiveness is being questioned since it has the potential to entrench biassed policing tactics[2]. In China, AI police systems use advanced surveillance technology and AI-powered analytics to follow residents and predict criminal conduct, but they frequently operate without clear legal protections, creating major human rights concerns[3].

Bangladesh, a developing country with a dynamic legal and technical environment, is rapidly exploring the possibility of using artificial intelligence into its criminal justice system. Although the current deployment is in its early phases, the government's concentration on digital transformation, creative law enforcement, and data-driven governance suggests the prospect of AI integration[4]. Nonetheless, Bangladesh's unique sociopolitical context presents both potential and problems, including weak legal frameworks, limited resources, and chronic socioeconomic imbalances. This fact underlines the need of taking efforts to prevent reinforcing existing inequities, overcoming procedural protections, and losing public trust, rather than just addressing chronic concerns such as court backlog, transparency shortages, and corruption. To successfully navigate these complexities, technology must be used with caution in the framework of good governance.

Applying a comparative perspective, this study analyses the benefits and constraints of integrating AI into the criminal justice systems of the United States, the United Kingdom, and China, deriving important conclusions for Bangladesh. The study conducts a critical evaluation of how issues about bias, fairness, openness,

[1] *Stevenson M., Slobogin C.* (2020). Data and discretion: Why we should exercise caution around using the COMPAS algorithm in court. Stanford Rewired. https://law.stanford.edu/publications/data-and-discretion/.

[2] *Joh E. E.* (2020). Artificial intelligence and policing: First questions // Annual Review of Law and Social Science, 16. Pp. 359–377. https://doi.org/10.1146/annurev-lawsocsci-101518-042816.

[3] *Burrell J., Knox H., Obrock M.* (2021). Transparency and oversight of risk assessment tools in criminal justice // Criminal Justice Ethics, 40(1). Pp. 3–21. https://doi.org/10.1080/0731129X.2020.1812149.

[4] *Hasan M., Chowdhury R., Rahman M.* (2022). Smart policing initiatives and AI adoption in Bangladesh // Asian Journal of Law and Technology, 11(2). Pp. 55–74.

and accountability are addressed or ignored in these jurisdictions, assessing the consequences for developing countries with fledgling legal systems. The analysis intends to provide guidance to policymakers, legal professionals, and researchers in Bangladesh on the technological, legal, and ethical factors involved in the integration of AI in criminal justice, emphasising the need for governance models that may be tailored to local environment.

This study conducts a comprehensive systematic analysis of contemporary academic literature, policy papers, legal frameworks, and case studies published after 2020. The investigation centres on empirical research on algorithmic efficacy and bias, assessments of governance responses, and recommendations for responsible AI development and regulation. This type of approach enables a comprehensive understanding of AI's transformational potential and associated hazards, emphasising the basic importance of human rights and the rule of law in directing the deployment of AI technology. In this instance, the use of artificial intelligence in criminal justice systems presents both advantages and significant obstacles. While AI technologies have the potential to improve efficiency and justice, they also run the risk of repeating current disparities if not handled carefully. Cross-country comparisons across different circumstances reveal diverse experiences and regulatory reactions, providing key lessons for Bangladesh as it seeks to integrate AI solutions into its criminal justice system. This essay contributes to the worldwide discussion over the need of deploying AI as a force for justice rather than oppression, particularly in the poor countries.

2. COMPAS in the United States: the reality of risk assessment algorithms

2.1. Overview and Adoption

COMPAS, or Correctional Offender Management Profiling for Alternative Sanctions, is a proprietary risk assessment tool utilised extensively in US court systems to guide bail, sentencing, and parole decisions. Despite its widespread use, academic researchers[1] and policymakers[2] have criticised COMPAS' black box approach and hidden structure. Because the underlying algorithm is proprietary, the relative weighting of the various factors; age, criminal history, and socioeconomic variables is opaque, making it impossible for courts or defendants to challenge or interpret the output scores[3].

[1] Wired. (2024). Judges are using algorithms to justify doing what they already want.

[2] *Stevenson M., Slobogin C.* (2020). Data and discretion: Why we should exercise caution around using the COMPAS algorithm in court. Stanford Rewired. https://law.stanford.edu/publications/data-and-discretion/.

[3] Ibid.

2.2. Accuracy and Prejudice Challenges

Several studies have found racial discrepancies in COMPAS test-prediction scores. In Broward County, for example, black non-recidivating offenders were mistakenly labelled as high risk nearly twice as often as white non-recidivating defendants (44.9% vs. 23.5%), but overall test-prediction accuracy across racial categories remained equal[1]. More broadly, risk assessment instruments have been criticised; recent studies suggest that even when arrest records are used as proxies for criminal behaviour, Black people have risk scores that are 0.5–2.8 percentage points higher, whereas when unobserved criminal behaviour is artificially included, this gap widens to between 4.5 and 11.0 percentage points[2].

2.3. Clarity and Fairness in Processes

The lack of openness incorporated into COMPAS undermines procedural fairness. According to Stevenson and Slobogin[3], judges must actively enquire to grasp the weighing of factors; unfortunately, most judges do not do so, resulting in "decisional blindness". Courts are typically just given a vague advice concerning COMPAS' proprietary restriction, rather than a full explanation of score computation[4]. Commentators have expressed worry that the theoretical foundations of these models may no longer be consistent with current behavioural patterns, particularly if algorithmic structures are not evaluated on a regular basis[5].

2.4. Judicial Conduct and Biassed Prosecution

Despite the availability of technologies such as COMPAS, judges may employ them selectively. According to recent study, judges are more likely to use algorithmic assessments to confirm decisions they are already inclined to make, particularly in lower-severity cases, while exercising greater caution in more serious instances. This restricted use does nothing to eradicate human bias and raises the possibility of utilising algorithms as a fig leaf to legitimise current judgements.

2.5. The Effects on Fairness Interpretations

Different fairness metrics, such as predictive parity and equal false positive rates, are mathematically incompatible in real data distributions. The COMPAS program

[1] *Dressel J., Farid H.* (2018). The accuracy, fairness, and limits of predicting recidivism // Science Advances, 4(1). e aao5580. https://doi.org/10.1126/sciadv.aao5580.

[2] *Zilka M., Fogliato R., Hron J., et al.* (2023). The progression of disparities within the criminal justice system: Differential enforcement and risk assessment instruments. arXiv.

[3] *Stevenson M., Slobogin C.* (2020). Data and discretion: Why we should exercise caution around using the COMPAS algorithm in court. Stanford Rewired. https://law.stanford.edu/publications/data-and-discretion/.

[4] Ibid.

[5] *Desmarais S., et al.* (2020). Broader issues surrounding model transparency in criminal justice risk scoring // Harvard Data Science Review.

cannot fulfil all fairness requirements at the same time, and decisions on which metric to employ are based on normative rather than technical reasoning. Thus, the illusion of fairness may obscure more basic inequalities contained in algorithmic design.

3. Predictive policing in the UK and AI-powered surveillance in CHINA

3.1. Predictive Policing in the UK

Predictive policing in the United Kingdom has been a key law enforcement breakthrough, using artificial intelligence (AI) and data analysis to look ahead and prevent crime. In contrast to traditional reactive policing, which responds to crime only after it occurs, predictive policing seeks to forecast criminality before it occurs, allowing police to adequately resource themselves and proactively prevent offending[1].

In the United Kingdom, predictive policing technology is often used to analyse datasets such as crime reports, arrest records, and sociodemographic information. For example, predictive crime mapping computer algorithms identify geographic hotspots where crime is likely to occur, whereas more advanced individual risk assessment systems seek to forecast people who are likely to conduct or become victims of crime[2]. However, their usage is still in its infancy as compared to nations such as the United States, and both their effectiveness and ethical concerns are being extensively explored.

The British government has become more aware of the risks associated with algorithmic policing. The UK government's advisory department, the department for Data Ethics and Innovation, has produced a number of publications emphasising the importance of openness, justice, and accountability in the use of AI-powered systems in police[3]. The CDEI 2020 assessment recommends that police algorithms be compliant with existing equality laws, particularly the Equality Act 2010, to prevent unlawful discrimination based on race, ethnicity, and socioeconomic position.

Amnesty International UK published a 2025 study titled Automated Racism, which is a critical analysis of predictive police technology used in the UK. According

[1] Centre for Data Ethics and Innovation. (2021a). Interim report: Review into bias in algorithmic decision-making. GOV.UK. https://www.gov.uk/government/publications/interim-report-review-into-bias-in-algorithmic-decision-making.

[2] Centre for Data Ethics and Innovation. (2021b). Ethics and governance of AI for policing: Public consultation. GOV.UK. https://www.gov.uk/government/consultations/ethics-and-governance-of-ai-for-policing-public-consultation.

[3] Centre for Data Ethics and Innovation. (2020). CDEI publishes review into bias in algorithmic decision-making. GOV.UK. https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making.

to the paper, at least 33 police departments have integrated predictive algorithms into their operational frameworks. While they have been advertised as more effective and crime-prevention tools, the systems will rely on databases like as stop-and-search data and arrest records, which disproportionately reflect policing prejudices against Black and ethnic minority communities[1]. This maintains a loop in which already overpoliced populations face more monitoring, leading to claims of racial profiling and institutionalised racism.

The highly decentralised nature of predictive policing raises serious concerns. While some police departments, such as the West Midlands Police, have formed data ethics panels to monitor the use of AI software, there is no national standard or regulatory environment for these technologies. This lack of standardisation raises the possibility of inconsistent practice and potential exploitation between countries. It also makes it difficult for the public to be confident that law enforcement officials be held accountable for choices made or based on AI systems.

3.2. UK's Ethical and Legal Concerns

The UK's ethical issues about predictive policing include openness, equality, and due process. Algorithms are "black boxes" in the sense that they make decisions that people, including law enforcement officials, cannot understand. Such opacity undermines the norms of procedural fairness and accountability in criminal justice. When people are subjected to increasing monitoring or intervention based on algorithmic predictions, they are unable to contest such measures or grasp the evidence against them. In response, the UK government and civil society groups have emphasised how important it is to incorporate ethical principles into AI development and uses. Additionally, the CDEI is developing a Code of Practice that will provide guidelines for the responsible use of algorithmic tools by public sector organisations, including law enforcement[2]. This law promotes thorough human judgement in decision-making, frequent result verification, and rigorous testing of algorithms against bias. Predictive policing data must be proportional, legally obtained, and subject to access and rectification rights, according to guidelines on data protection principles in AI released by the UK Information Commissioner's Office (ICO)[3].

[1] Amnesty International UK. (2025). Automated racism: How police data and algorithms code discrimination into policing. Amnesty International UK.

[2] Centre for Data Ethics and Innovation. (2021a). Interim report: Review into bias in algorithmic decision-making. GOV.UK. https://www.gov.uk/government/publications/interim-report-review-into-bias-in-algorithmic-decision-making.

[3] Information Commissioner's Office. (2021). Guide to data protection. ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/.

However, when these programs are implemented, objective reviews have noted a lack of strong empirical evidence that predictive policing improves crime levels in the UK[1]. There are also fears that the system may exacerbate present social imbalances. The prospect of bias in algorithms is particularly significant since training data sets repeat past policing inequities, making it impossible to discriminate between true crime trends and biassed enforcement patterns[2].

3.3. AI-Powered Surveillance in China

China follows a distinct paradigm of AI use in criminal justice and public security, with widespread deployment of AI-facilitated surveillance integrated into official institutions of governance and social control. The Chinese government has made major expenditures in surveillance technology such as closed-circuit television (CCTV) cameras with facial recognition, AI-powered data processing, and social credit scoring processes[3].

According to Human Rights Watch (2020), Chinese police employ "Big Data" technologies to follow people and groups by collecting and analysing biometric data, online activity, movement history, and even speech recognition. The devices are primarily employed to detect and crush opposition among ethnic minorities, like as the Uighurs in Xinjiang region. Sensitive face recognition criteria classify persons based on racial and ethnic characteristics, allowing for easy targeted monitoring and control[4].

China's surveillance AI systems operate on a massive scale, with no public exposure or judicial control. To demonstrate, the "police cloud" system combines data from many sources to create detailed profiles of individuals, estimating their risk and possible harm to societal stability[5]. The system may take law enforcement action based on AI projections of the person's behaviour, social networks, and political involvement, with no obvious legal protections or routes for review. This particular kind of technology is an important component of China's "techno-authoritarian" governance style, which prioritises

[1] Amnesty International UK. (2025). Automated racism: How police data and algorithms code discrimination into policing. Amnesty International UK.

[2] *Fussey P., Murray D.* (2021). Predictive policing: An ethics and human rights assessment // Policing and Society, 31(1). Pp. 34–48. https://doi.org/10.1080/10439463.2020.1713182.

[3] *Creemers R.* (2020). China's social credit system: An evolving practice of control. SSRN. https://doi.org/10.2139/ssrn.3425790.

[4] Reuters. (2021, March 30). China found using surveillance firms to help write ethnic-tracking specs. Reuters. https://www.reuters.com/article/us-china-surveillance-idUSKBN2BM1VQ.

[5] *Doffman Z.* (2023). China's surveillance technology is keeping tabs on populations around the world. Forbes. https://www.forbes.com/sites/zakdoffman/2023/02/21/chinas-surveillance-technology/.

state security above widespread monitoring and control[1]. Unlike the United Kingdom, China prioritises regime stability and social control over balancing public safety with individual liberty. This has significant human rights implications for privacy, freedom of speech, and protection against arbitrary imprisonment.

3.4. Legal and Human Rights Issues in China

In China, limited legislative safeguards exist to protect individual rights against AI-based monitoring. Existing rules give law enforcement vast authority, there is little court oversight or independent monitoring, and AI algorithms are not transparent, further restricting accountability. People are typically unaware of the grounds for their imprisonment or monitoring[2]. International observers have condemned China's AI-based monitoring as systematic discrimination and a breach of international human rights legislation[3]. Algorithmic sorting aimed at ethnic minorities increases the risk of racial profiling and cultural repression. Furthermore, the use of AI for social credit scoring, which scores persons' trustworthiness based on behaviour, raises ethical concerns about algorithmic governance and mass social control.

3.5. Comparing UK and Chinese AI Policing Models

The differences between the UK and China's implementations of AI in criminal justice reflects contrasting political, legal, and cultural circumstances that influence technological adoption.

The UK model is distinguished by careful experimentation with predictive policing within a democratic setting that prioritises rule of law, openness, and human rights protection. Recognising the ongoing concerns of bias and accountability, there is increasing institutional recognition of the need for ethical AI system governance, including independent review and public participation[4]. Individuals can appeal algorithmic judgements under the UK's multiple legal frameworks, but operational impediments still exist.

China's AI-powered monitoring operates under a centralised, authoritarian government that prioritises societal stability and regime security over individual

[1] *Liang F., Das V., Kostyuk N., Hussain M.M. (*2021). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure // Policy & Internet, 13(4). Pp. 415–453. https://doi.org/10.1002/poi3.259.

[2] Human Rights Watch. (2020). China: Police "big data" systems violate privacy, target dissent. https://www.hrw.org/news/2020/01/17/china-police-big-data-systems-violate-privacy.

[3] Ibid.

[4] Centre for Data Ethics and Innovation. (2021b). Ethics and governance of AI for policing: Public consultation. GOV.UK. https://www.gov.uk/government/consultations/ethics-and-governance-of-ai-for-policing-public-consultation.

liberties[1]. Surveillance technologies are currently being implemented on an unprecedented scale and are deeply integrated in daily life, with little transparency or accountability[2]. The use of racial and ethnic data by the state to spy and target minority groups raises serious ethical and human rights problems[3].

These diverse models raise important considerations concerning the role of governance institutions and legal standards in determining the use of AI technology in criminal justice. Democratic societies will prioritise procedural justice and civil rights, requiring AI systems that are intelligible, contestable, and subject to monitoring. Authoritarian cultures will prioritise societal order, using AI to monitor and govern with fewer checks and balances.

3.6. Lessons and Implications for Bangladesh

The use of AI in criminal justice is a topic that Bangladesh's legal system is only beginning to address, but there are lessons to be learnt from China's and the UK's experiences. Bangladesh must weigh the potential advantages of AI, such as better resource allocation and crime prevention, against the dangers of prejudice, discrimination, and the degradation of basic rights.

The significance of integrating AI technologies into a process for transparency, ethical regulation, and legal safeguarding is highlighted by the UK experience. Lawmakers in Bangladesh must prioritise enacting regulations that control the collection and use of data, require algorithm transparency, and set up strict accountability procedures. Building confidence in AI-driven law enforcement operations also requires public knowledge and engagement. On the other hand, the Chinese model highlights the risks associated with AI spying in the absence of privacy and human rights protections. Techno-authoritarian strategies that increase state authority without preserving democratic balance should not be imitated by Bangladesh. Rather, the use of AI must be carried out in a way that respects due process, human dignity, and the prevention of prejudice.

Bangladesh needs to develop institutional capacity in order to responsibly harness the potential of AI. This includes establishing independent advisory bodies, data ethics committees, and technological capabilities for AI fairness. Civil society, academics, and international human rights organisations may help Bangladesh create governance structures that are appropriate for its culture and the law.

[1] *Liang F., Das V., Kostyuk N., Hussain M.M. (*2021). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure // Policy & Internet, 13(4). Pp. 415–453. https://doi.org/10.1002/poi3.259.

[2] *Doffman Z.* (2023). China's surveillance technology is keeping tabs on populations around the world. Forbes. https://www.forbes.com/sites/zakdoffman/2023/02/21/chinas-surveillance-technology/.

[3] Reuters. (2021, March 30). China found using surveillance firms to help write ethnic-tracking specs. Reuters. https://www.reuters.com/article/us-china-surveillance-idUSKBN2BM1VQ.

4. Key challenges in algorithmic criminal justice: Bias, Fairness, Due Process, and Transparency

4.1. Algorithmic Bias and the Cause

Artificial intelligence criminal justice systems reflect and exaggerate built-in prejudices in today's societal biases that are included into their training data[1]. Because AI models are designed based on historical crime and court records, the algorithm may incorporate and perpetuate police or sentencing disparities caused by institutional racism, class prejudice, or sociopolitical inequities[2]. For example, disproportionate minority community arrests in databases distort predictive police and risk assessments, forming "feedback loops" that reinforce biassed judgements.

Recent research has shown that even 'neutral' characteristics can function as proxies for race, gender, or economic status, resulting in indirect discrimination. Furthermore, algorithmic judgements often disproportionately damage marginalised groups, increasing social inequities under the guise of 'objectivity'. The opaque nature of commercial AI systems makes it difficult to identify and address such biases[3].

4.2. Different Measures of Fairness and Their Limitations

Algorithmic criminal justice fairness is difficult and contentious, with several measurements giving opposing viewpoints. Traditional fairness notions include demographic parity, equalised odds, and calibration[4]. These requirements are mutually incompatible in operation; no single model can meet all of the fairness criteria at the same time. The optimal choice of whatever fairness indicator to target becomes a normative, policy-related issue rather than merely technical.

COMPAS, for example, exhibits this trade-off: it predicts recidivism equally well in both racial groups but produces more false positives in Black offenders[5] Equally prioritising false positives reduces overall predictiveness, whereas equitably prioritising calibration reinforces race-based inequities[6].

Recent study emphasises that fairness must be considered contextually based on social and legal criteria, as well as the cumulative impact on the affected

[1] *Berk R., Heidari H., Jabbari S., Kearns M., Roth A.* (2021). Fairness in criminal justice risk assessments: The state of the art // Sociological Methods & Research.

[2] *Lum K., Isaac W.* (2016). To predict and serve? // Significance, 13(5). Pp. 14–19.

[3] *Larson J., Mattu S., Kirchner L., Angwin J.* (2016). How we analyzed the COMPAS recidivism algorithm. ProPublica.

[4] *Chouldechova A.* (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments // Big Data, 5(2). Pp. 153–163. https://doi.org/10.1089/big.2016.0047.

[5] *Angwin J., Larson J., Mattu S., Kirchner L.* (2016). Machine bias. ProPublica. (In English)

[6] *Chouldechova A.* (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments // Big Data, 5(2). Pp. 153–163. https://doi.org/10.1089/big.2016.0047.

populations[1]. To address these tensions, open stakeholder involvement and impact assessments are required[2].

4.3. Due Process and Transparency Challenges

Algorithmic justice methods in criminal cases typically lose procedural fairness by making choices vague[3]. Defendants may get unfavourable decisions based on opaque risk ratings without awareness of the data or methodology used to create the rankings, preventing them from contesting or comprehending the evidence against them[4]. This "black-box" behaviour violates principles of due process, legal openness, and accountability.

Courts throughout the world are trying to figure out how to balance AI usage with constitutional protection. For example, under the General Data Protection Regulation (GDPR), European Union legal frameworks increasingly require explainability and data subject rights, such as limits on automated decision-making[5]. The majority of US jurisdictions, on the other hand, lack consistent regulation, resulting in different algorithmic review requirements[6].

To improve transparency, proposed recent initiatives call for "algorithmic impact assessments" that thoroughly investigate potential harms and benefits ahead of time, as well as legal audits and public disclosure of model design and output[7]. The evaluations should also take into account the viewpoints of impacted groups in order to prevent the concentration of already-existing imbalances under technological control.

4.4. Accountability and human surveillance

Human judgement is vital to criminal justice, but it is increasingly influenced by computer advice. Mechanisms for accountability lag behind technological

[1] *Hajian S., Bonchi F., Castillo C.* (2021). Algorithmic bias: From discrimination discovery to fairness-aware data mining // ACM SIGKDD Explorations Newsletter, 21(1). Pp. 14–27. https://doi.org/10.1145/3457309.3457312.

[2] *Raji I. D., Smart A., White R. N., Mitchell M., Gebru T.* (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing // Proceedings of the Conference on Fairness, Accountability, and Transparency.

[3] *Citron D. K., Pasquale F.* (2019). The scored society: Due process for automated predictions // Washington Law Review, 89(1). Pp. 1–33.

[4] *Barabas C., Dinakar K., Ito J., et al.* (2020). Interventions over predictions: How to use AI to help humans make better decisions // Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society.

[5] *Goodman B., Flaxman S.* (2017). European Union regulations on algorithmic decision-making and a "right to explanation" // AI Magazine, 38(3). Pp. 50–57.

[6] *Stevenson M., Slobogin C.* (2020). Data and discretion: Why we should exercise caution around using the COMPAS algorithm in court. Stanford Rewired. https://law.stanford.edu/publications/data-and-discretion/.

[7] *Diakopoulos N.* (2019). Automating the news: How algorithms are rewriting the media. Harvard University Press.

advances[1]. Overreliance on AI risks creating "automation bias", in which human decision-makers accept algorithmic suggestions without question, transferring responsibility and undermining professional judgement[2].

Accountability models must explicitly define the responsibilities of developers, deployers, and AI system adjudicators[3]. Judicial training, for example, is required to ensure that judges understand algorithmic bias and perceive risk rankings as advisory rather than determinative[4]. When damage occurs, regulatory organisations must guarantee auditability, openness, and routes for remedy[5].

4.5. Ethical and Social Implications

The use of AI in criminal justice raises basic ethical problems about equality, justice, and technology's role in societal control[6]. Algorithmic platforms may rationalise punitive actions under the guise of scientific authority, reinforcing systemic inequities and disproportionately monitoring disadvantaged communities[7] Scholars urge for putting human rights, social justice, and democratic involvement at the forefront of AI governance frameworks[8]. These include including justice "by design", continuously tracking unequal affects, and integrating numerous stakeholders in creation and regulation[9].

4.6. Significance in Bangladesh

These challenges are particularly serious in Bangladesh. New AI adoption in an evolving judicial system with limited data privacy and institutional capacity

[1] *Joh E. E.* (2020). Artificial intelligence and policing: First questions // Annual Review of Law and Social Science, 16. Pp. 359–377. https://doi.org/10.1146/annurev-lawsocsci-101518-042816.

[2] *Gunning D.* (2019). Explainable artificial intelligence (XAI). Defense Advanced Research Projects Agency (DARPA).

[3] *Diakopoulos N.* (2019). Automating the news: How algorithms are rewriting the media. Harvard University Press.

[4] *Stevenson M., Slobogin C.* (2020). Data and discretion: Why we should exercise caution around using the COMPAS algorithm in court. Stanford Rewired. https://law.stanford.edu/publications/data-and-discretion/.

[5] *Raji I. D., Smart A., White R. N., Mitchell M., Gebru T.* (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing // Proceedings of the Conference on Fairness, Accountability, and Transparency.

[6] *Eubanks V.* (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press.

[7] *Benjamin R.* (2019). Race after technology: Abolitionist tools for the new Jim code. Polity Press.

[8] *Mayson S.* (2021). Bias in, bias out: Algorithmic fairness and the limits of policy // Yale Law Journal, 130(8). Pp. 2140–2210. https://doi.org/10.2139/ssrn.3478377.

[9] *Binns R.* (2020). Fairness in machine learning: Lessons from political philosophy // Proceedings of the Conference on Fairness, Accountability, and Transparency.

might worsen current justice disparities[1]. Bangladesh may be forced to adopt defective models that undermine due process and human rights if algorithmic bias, transparency, and accountability are not regulated. As a result, a conservative, contextualised strategy that prioritises openness, community participation, and capacity building is required. Bangladesh demands adaptive AI governance solutions that strike a balance between technology development and basic legal and ethical protections.

5. Sentencing algsorithms: comparative analysis and opportunities and challenges for Bangladesh

5.1. Introduction to sentence algorithms

Sentencing algorithms are currently a key use of artificial intelligence in global criminal justice systems. Algorithms are used to analyse defendant data and criminal histories, generating risk ratings or recommendations that impact sentence, parole eligibility, and bail[2]. The purported benefits include more uniformity, less human discretion, and improved efficiency in courts that have traditionally been burdened by case backlogs and discretionary variation[3]. Having said that, the deployment of such algorithms raises complicated legal, ethical, and societal considerations that necessitate extensive comparative examination.

5.2. The United States: COMPAS and its controversies

The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is the most extensively investigated sentencing tool, and it was predominantly used in various US states to estimate the likelihood of recidivism[4] (Angwin et al., 2016). COMPAS, instead of reducing sentencing disparity, has been accused of aggravating racial prejudice. Research demonstrates that Black defendants are more likely to be misclassified as high risk, whereas White defendants are more likely to be mislabelled as low risk[5]. In response to such criticism, American lawmakers and courts have begun to challenge the admissibility

[1] *Talukder K. A., Shompa T. F.* (2023). Artificial intelligence in criminal justice management: A systematic literature review // Journal of Machine Learning, Data Engineering and Data Science.

[2] *Dressel J., Farid H.* (2018). The accuracy, fairness, and limits of predicting recidivism // Science Advances, 4(1). e aao5580. https://doi.org/10.1126/sciadv.aao5580.

[3] *Ferguson A. G.* (2020). The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press.

[4] *Angwin J., Larson J., Mattu S., Kirchner L.* (2016). Machine bias. ProPublica.

[5] *Dressel J., Farid H.* (2018). The accuracy, fairness, and limits of predicting recidivism // Science Advances, 4(1). e aao5580. https://doi.org/10.1126/sciadv.aao5580.

of COMPAS scores on the grounds of transparency, the algorithm's proprietary nature severely limits examination and violates defendants' due process rights[1]. Furthermore, although some countries use algorithmic proposals on a locutionary scale as a guideline, others increasingly rely on these ratings to determine punishment, thereby entrenching systemic biases inside institutionalised courts of law[2].

5.3. UK: sentencing and risk assessment tools

The United Kingdom uses a variety of AI technologies to influence sentencing decisions and probation services, highlighting rehabilitation potential and reoffending risk. The Offender Assessment System (OASys) is a structured professional judgement tool with algorithmic scoring that informs sentence and monitoring programs[3]. In contrast to COMPAS, OASys incorporates more qualitative feedback from probation officials and combines human judgement with data analysis.

Nonetheless, there is ongoing concern that such systems will be erroneous, biassed, and opaque. Opponents say that risk evaluations will disproportionately affect ethnic and socioeconomically disadvantaged populations, mirroring difficulties in the US environment. The legislation in the United Kingdom has to be more open, since courts require disclosure of algorithmic practice in sentencing cases. The legal environment fosters the prudent, measured use of AI technologies while increasing judicial discretion[4].

5.4. China's surveillance-driven sentencing environment

China's criminal justice usage of AI differs from Western applications in that it includes risk assessment as part of a large monitoring system[5]. Sentencing judgements frequently use AI-predicted behavioural profiles obtained from surveillance data alongside traditional legal factors. This "social credit" deployment evaluates an individual's "trustworthiness" and "social stability" as predictors of punishment harshness and parole[6]. While there is official restraint on transparency, reports

[1] *Stevenson M., Slobogin C.* (2020). Data and discretion: Why we should exercise caution around using the COMPAS algorithm in court. Stanford Rewired. https://law.stanford.edu/publications/data-and-discretion/.

[2] *Ferguson A. G.* (2020). The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press.

[3] *Burrell J., Knox H., Obrock M.* (2021). Transparency and oversight of risk assessment tools in criminal justice // Criminal Justice Ethics, 40(1). Pp. 3–21. https://doi.org/10.1080/0731129X.2020.1812149.

[4] Ibid.

[5] Human Rights Watch. (2020). China: Police "big data" systems violate privacy, target dissent. https://www.hrw.org/news/2020/01/17/china-police-big-data-systems-violate-privacy.

[6] *Zeng W., Li H., Shi Q.* (2022). AI surveillance and social credit in China: Implications for criminal justice // Journal of Asian Public Policy, 15(1). Pp. 47–66.

show that data obtained from AI-based surveillance, such as facial recognition, communications monitoring, and public behaviour analysis, is fed into sentencing algorithms capable of overriding evidence standards or judicial discretion[1]. The merging of AI with authoritarian legal paradigms heightens concerns about due process abuses, political repression, and a lack of justice for people who have been unfairly targeted[2].

5.5. Growing interest in sentencing algorithms in Bangladesh

Bangladesh is still in the early stages of using AI in its criminal justice system. Nonetheless, increased attention from politicians and technologists indicates that sentencing algorithms will be used soon to reduce judicial delay, varied punishment, and jail overcrowding[3]. The government has made investments in "smart policing" efforts including data analytics, and there is rising discussion regarding the use of AI to improve court efficiency[4]. Despite this sense of anticipation, Bangladesh faces formidable hurdles. For starters, data quality and availability remain poor, with disparate criminal records and inconsistent reporting across jurisdictions. Second, legislative measures for data security, transparency, and accountability are still in their infancy; the Personal Data security Act is young and lacks provisions for AI and automated decision-making.

5.6. Challenges to fair and ethical AI adoption in Bangladesh

The use of sentencing algorithms in the absence of strong legal and institutional frameworks risks reinforcing existing inequities. Bangladesh's courts are already susceptible to sociopolitical meddling, corruption, and shortages, which AI may accidentally exacerbate if not regulated[5]. Algorithmic prejudice can amplify systemic biases against marginalised groups including indigenous peoples and religious minorities[6]. Furthermore, court personnel may lack the technical skills required to critically analyse AI suggestions, increasing the risk of automation bias

[1] *Zeng W., Li H., Shi Q.* (2022). AI surveillance and social credit in China: Implications for criminal justice // Journal of Asian Public Policy, 15(1). Pp. 47–66.

[2] Human Rights Watch. (2020). China: Police "big data" systems violate privacy, target dissent. https://www.hrw.org/news/2020/01/17/china-police-big-data-systems-violate-privacy.

[3] *Talukder K. A., Shompa T. F.* (2023). Artificial intelligence in criminal justice management: A systematic literature review // Journal of Machine Learning, Data Engineering and Data Science.

[4] *Hasan M., Chowdhury R., Rahman M.* (2022). Smart policing initiatives and AI adoption in Bangladesh // Asian Journal of Law and Technology, 11(2). Pp. 55–74.

[5] *Rahman T.* (2021). Corruption, inefficiency, and reforms in Bangladesh criminal justice // Bangladesh Journal of Law, 15(1). Pp. 98–117.

[6] *Ahmed S., Khan M.* (2020). Social justice and discrimination in Bangladesh: Challenges for marginalized groups // Journal of South Asian Studies, 38(3). Pp. 411–428.

and overreliance on algorithmic outputs[1]. Without accountability and auditing systems, defendants would be increasingly unable to contest AI-based judgements, jeopardising core due process safeguards.

5.7. Opportunity for responsible AI integration

Despite these concerns, Bangladesh has the potential to employ AI responsibly by learning from worldwide best practices. Some of the key recommendations are:

— Data Governance and Quality Improvement: Establishing uniform, safe, and accessible criminal data repositories to ensure AI technologies employ credible, representative datasets[2]

— Legal and regulatory frameworks: Adopting comprehensive AI-specific regulations to provide openness, fairness, and accountability in conformity with international human rights norms.

— Capacity Building: Educating judges, prosecutors, and law enforcement officials on AI's capabilities and limits in order to encourage critical oversight and informed decision-making[3].

— Algorithmic Impact Assessments: Conducting independent pre-deployment testing to identify and reduce biases or harms, including interaction with marginalised community stakeholders[4].

— Transparency and Explainability: Ensure that AI sentencing technologies produce explainable results for scrutiny by relevant parties and courts[5].

5.8. Summary and Future Directions

Sentencing algorithms have both potential and risk. Comparative experiences from the US, UK, and China show that, while AI has the ability to improve judicial efficiency and impartiality, careless design and regulation have the potential to intensify prejudice, violate due process, and reduce public faith in legal institutions. For Bangladesh, the route forward must involve intentional, context-driven policies that balance AI deployment with democratic principles and human rights. Investment in data infrastructure, legal reform, capacity building, and inclusive governance may alleviate dangers while also leveraging AI's promise to improve criminal justice results.

[1] *Talukder K. A., Shompa T. F.* (2023). Artificial intelligence in criminal justice management: A systematic literature review // Journal of Machine Learning, Data Engineering and Data Science.

[2] *Hasan M., Chowdhury R., Rahman M.* (2022). Smart policing initiatives and AI adoption in Bangladesh // Asian Journal of Law and Technology, 11(2). Pp. 55–74.

[3] *Rahman T.* (2021). Corruption, inefficiency, and reforms in Bangladesh criminal justice // Bangladesh Journal of Law, 15(1). Pp. 98–117.

[4] *Burrell J., Knox H., Obrock M.* (2021). Transparency and oversight of risk assessment tools in criminal justice // Criminal Justice Ethics, 40(1). Pp. 3–21. https://doi.org/10.1080/0731129X.2020.1812149.

[5] *Mayson S.* (2021). Bias in, bias out: Algorithmic fairness and the limits of policy // Yale Law Journal, 130(8). Pp. 2140–2210. https://doi.org/10.2139/ssrn.3478377.

6. Policy recommendations and governance frameworks for AI in criminal justice: Bangladesh perspective

6.1. The need for policy and governance

The growing integration of artificial intelligence (AI) into criminal justice systems throughout the world emphasises the critical need for robust governance frameworks to guarantee that these technologies are used ethically, openly, and accountable. Bangladesh, as a develpoing country on the threshold of implementing AI in its criminal justice system, has unique hurdles. They have underdeveloped legal frameworks, little institutional capacity, and complicated sociopolitical environments, all of which increase the potential of AI misuse and abuse. Without carefully planned regulations and governance structures, AI has the potential to exacerbate existing socioeconomic inequities, undermine public trust in justice systems, and violate basic rights. As a result, it is Bangladesh's obligation to proactively develop governance frameworks that are tailored to its specific environment, maximising the potential advantages of AI while minimising any risks.

6.2. Fundamental principles for AI governance in criminal justice

A successful governance framework for AI in Bangladesh's criminal justice system must be based on a set of fundamental principles derived from both global best practices and local circumstances. First and foremost, non-discrimination and justice must be prioritised, so that AI systems do not perpetuate or acquire bias against marginalised populations such as ethnic minorities, women, and the economically poor. Transparency and explainability are also required to ensure that AI methodologies, decision-making variables, and data sources are publicly revealed so that people impacted, legal experts, and the general public may understand and, if necessary, dispute AI-based choices. Accountability is another important premise; clearly defined duties should be allocated to AI developers, law enforcement, the courts, and regulators, with accessible channels for grievance redressal and remedies. Data protection and privacy precautions must also be consistent with strict legal standards in order to avoid abuse, unauthorised access, and intrusive profiling. Maintaining human monitoring is also necessary to ensure that AI remains a tool to supplement, rather than replace, judicial judgement, and to avoid over-reliance on machine-generated recommendations. Finally, stakeholder input, including marginalised populations, civil society, technologists, and legal experts, must be integrated into AI design, deployment, and monitoring to ensure inclusion and responsiveness.

6.3. Establishing legal and regulatory infrastructur

Bangladesh currently lacks a specific legal framework for the application of AI, notably in the sensitive field of criminal justice. To close this gap, Bangladesh should create thorough AI law that establishes explicit requirements for algorithmic fairness, transparency, data governance, and accountability in accordance with international human rights duties. The legislation should clearly state what applications of AI in criminal justice are permitted and which are not. It should also require rigorous algorithmic impact assessments prior to deployment, public disclosure of AI system design and performance metrics, stringent data privacy safeguards in accordance with existing data protection laws, and clear arrangements for human oversight and judicial review of AI-generated decisions. Simultaneously, Bangladesh's data protection policy, which is still in its early stages, should be tightened to address AI-specific concerns such as automated profiling and mass monitoring. This can be accomplished by amending the Personal Data Protection Act with detailed provisions on data minimisation, purpose limitation, data access and correction rights, restrictions on international data transfers, and data controller obligations to prevent discriminatory outcomes in AI systems. Furthermore, independent monitoring organisations with technical and legal competence must be formed to oversee AI deployment in criminal justice. These regulators would be in charge of conducting frequent audits for bias and accuracy, investigating complaints, providing advice and certification for AI tools, and promoting public openness through reporting and public participation. Bangladesh might take inspiration from models such as the UK's Centre for Data Ethics and Innovation and the European Union's planned AI regulatory framework for guidance on how to create such organisations.

6.4. Building institutional and technical capacity

To be effective, AI governance in Bangladesh requires enormous investment in capacity building across several domains. Judges and legal professionals must get training so that they can critically analyse AI output, comprehend algorithmic evidence, and appropriately defend defendants' rights. Police personnel and prosecutors must be schooled in ethical data usage, privacy rules, and the limitations of AI systems in order to avoid abusing them. Equally crucial is teaching AI engineers and data scientists in legal compliance and fairness-aware design principles, so that technology producers are mindful of the ethical consequences of their products. Policymakers and regulators must get continual briefings on new AI trends, related dangers, and governance solutions in order to make educated and successful policy decisions. Bangladesh must also modernise its data infrastructure by developing integrated, digitised criminal justice databases that contain high-quality, standardised data. This includes creating privacy-protecting safe data storage and sharing agreements, as well as conducting thorough data quality checks to reduce bias and mistakes that weaken AI performance and fairness.

6.5. Ensuring transparency and public engagement

Transparency is critical for establishing public confidence and legitimacy for AI usage in criminal justice. Bangladesh should require that AI techniques used in this context produce explainable, interpretable outputs that are available to defendants and their counsel, allowing them to understand the reasoning behind risk estimations or sentence recommendations. Furthermore, algorithmic effect evaluations, such as bias audits and mistake rates, should be made available in clearly comprehensible formats. Public consultations and community seminars are also necessary to obtain feedback from a varied variety of stakeholders, raise awareness of AI's role and hazards, and ensure that various viewpoints shape governance frameworks. Civil society organisations and academic institutions should be encouraged to actively participate in supervision, research, and advocacy initiatives, resulting in a diverse governance environment that combines technical competence with social accountability.

6.6. Promoting ethical AI design and use

Ethical AI design involves incorporating principles such as justice, accountability, and respect for human rights throughout the technological development lifecycle. This includes using fairness-aware machine learning approaches to actively uncover and eliminate biases, as well as updating models on a regular basis to reflect changing social circumstances and prevent prejudice. AI technology must be developed with "human-in-the-loop" features that enable automated output to supplement, rather than replace, human judgement, as well as systems for override and review. There must also be ongoing monitoring and feedback systems in place to evaluate AI performance in real-world scenarios and recalibrate models as needed. Furthermore, it is critical that AI technology be tailored to Bangladesh's cultural and contextual conditions rather than being adopted wholesale from other nations. This ensures that language, social conventions, and legal requirements are adequately accounted for in the design, hence enhancing accuracy and fairness.

6.7. International cooperation and knowledge exchange

Bangladesh may benefit considerably from international collaboration and information sharing in the regulation of AI in criminal justice. Bangladesh will be able to get access to technical knowledge, learn from the experiences of other nations, and align policy with widely accepted international norms by engaging in global initiatives such as the Global Partnership on AI and UNESCO's AI ethics work. Collaboration with human rights organisations will ensure that AI applications comply with global human rights standards. Furthermore, collaboration with academic and non-governmental organisations might help to co-create AI solutions that are not just creative but also socially responsible and adapted to the needs of Bangladesh.

6.8. Risks of inaction and the need for reform

If Bangladesh does not move quickly to regulate AI in criminal justice, it risks deepening structural biases in the legal system, exacerbating socioeconomic inequities and compromising due process and legal certainty. The improper use of AI will destroy public trust in justice systems, perhaps causing major social discontent and a loss of legitimacy. Given the rate of digitalisation, quick adjustments are required to avoid these harmful consequences. Advance policymaking and capacity building will not only safeguard rights and promote fairness, but will also position Bangladesh as a progressive and responsible leader in the field of AI-powered justice.

7. Conclusion

This study examined the use of artificial intelligence in criminal justice by doing a comparative examination of AI-powered technologies in the United States, the United Kingdom, and China, as well as their impacts on fairness, transparency, and accountability. Through case studies of predictive police software such as COMPAS, PredPol, and China's integrated surveillance systems, the research revealed the intricate relationship between technical innovation and fundamental legal concepts.

According to the study, while AI technologies have the potential to improve efficiency and impartiality in criminal justice, they also pose important problems about prejudice, due process, and equal treatment before the law. In practice, such technologies operate within and are influenced by the sociopolitical context in which they are deployed. As a result, they likely to repeat and even exacerbate existing inequities, particularly when datasets reflect historical injustices or institutional prejudice.

The UK assessment illustrates a cautious but increasingly systematic attempt to include algorithmic tools, which is frequently accompanied by efforts to establish ethical monitoring and public responsibility. In contrast, the Chinese instance shows broad use of AI technology with limited transparency and little consideration for individual rights, demonstrating how diverse political and legal regimes impact the development and use of AI in police. These comparisons emphasise the relevance of governance mechanisms in balancing the dangers and advantages of technology integration in criminal justice.

The research also assessed the relevance of such global achievements to the Bangladesh context. While Bangladesh is not yet actively involved in using AI in its judicial system, it will face the same challenges as other countries, particularly in terms of data governance, institutional preparation, and legal safeguards. The comparative analysis in this study provides an essential baseline for determining the potential impact of incorporating such technology in a growing judicial system.

One recurring topic throughout the research has been that the employment of AI in criminal justice systems must not jeopardise the fundamental principles that underpin the rule of law. AI can help with caseload management, risk assessment, and decision-making, but it cannot replace the crucial function of human judgement in interpreting context, exercising discretion, and achieving justice on an individual basis.

The article has shed light on the ways algorithmic decision-making might impact not just individual results but also institutional legitimacy and public confidence by summarising the main issues examined. Legal institutions that are already being weakened by inefficiency and injustice are especially vulnerable to the dangers of opaque, biassed, or unsupervised AI systems. Because of this, the use of AI in criminal justice necessitates ongoing evaluation, careful application, and conformity to legal norms that uphold individual liberties and encourage fair treatment under the law.

This study has demonstrated that the legal, ethical, and institutional decisions made by those who develop, implement, and oversee these technologies have an influence on criminal justice that is not neutral. Moreover, the study has demonstrated that the legal, ethical, and institutional decisions made by those who develop, implement, and oversee these technologies have a significant influence on how AI affects criminal justice.

References

Ahmed S., Khan M. (2020). Social justice and discrimination in Bangladesh: Challenges for marginalized groups // Journal of South Asian Studies, 38(3). Pp. 411–428. (In English)

Amnesty International UK. (2025). Automated racism: How police data and algorithms code discrimination into policing. Amnesty International UK. (In English)

Angwin J., Larson J., Mattu S., Kirchner L. (2016). Machine bias. ProPublica. (In English)

Atlantic Council. (202X). The West, China, and AI surveillance. (Precise year to be inserted). (In English)

Barabas C., Dinakar K., Ito J., et al. (2020). Interventions over predictions: How to use AI to help humans make better decisions // Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society. (In English)

Benjamin R. (2019). Race after technology: Abolitionist tools for the new Jim code. Polity Press. (In English)

Berk R., Heidari H., Jabbari S., Kearns M., Roth A. (2021). Fairness in criminal justice risk assessments: The state of the art // Sociological Methods & Research. (In English)

Binns R. (2020). Fairness in machine learning: Lessons from political philosophy // Proceedings of the Conference on Fairness, Accountability, and Transparency. (In English)

Burrell J., Knox H., Obrock M. (2021). Transparency and oversight of risk assessment tools in criminal justice // Criminal Justice Ethics, 40(1). Pp. 3–21. https://doi.org/10.1080/0731129X.2020.1812149. (In English)

Centre for Data Ethics and Innovation. (2020). CDEI publishes review into bias in algorithmic decision-making. GOV.UK. https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making. (In English)

Centre for Data Ethics and Innovation. (2021a). Interim report: Review into bias in algorithmic decision-making. GOV.UK. https://www.gov.uk/government/publications/interim-report-review-into-bias-in-algorithmic-decision-making. (In English)

Centre for Data Ethics and Innovation. (2021b). Ethics and governance of AI for policing: Public consultation. GOV.UK. https://www.gov.uk/government/consultations/ethics-and-governance-of-ai-for-policing-public-consultation. (In English)

Chouldechova A. (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments // Big Data, 5(2). Pp. 153–163. https://doi.org/10.1089/big.2016.0047. (In English)

Citron D.K., Pasquale F. (2019). The scored society: Due process for automated predictions // Washington Law Review, 89(1). Pp. 1–33. (In English)

Creemers R. (2020). China's social credit system: An evolving practice of control. SSRN. https://doi.org/10.2139/ssrn.3425790. (In English)

Desmarais S., et al. (2020). Broader issues surrounding model transparency in criminal justice risk scoring // Harvard Data Science Review. (In English)

Diakopoulos N. (2019). Automating the news: How algorithms are rewriting the media. Harvard University Press. (In English)

Doffman Z. (2023). China's surveillance technology is keeping tabs on populations around the world. Forbes. https://www.forbes.com/sites/zakdoffman/2023/02/21/chinas-surveillance-technology/. (In English)

Dressel J., Farid H. (2018). The accuracy, fairness, and limits of predicting recidivism // Science Advances, 4(1). eaao5580. https://doi.org/10.1126/sciadv.aao5580. (In English)

Eubanks V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press. (In English)

European Commission. (2021). Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. (In English)

Ferguson A. G. (2020). The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press. (In English)

Fussey P., Murray D. (2021). Predictive policing: An ethics and human rights assessment // Policing and Society, 31(1). Pp. 34–48. https://doi.org/10.1080/10439463.2020.1713182. (In English)

Goodman B., Flaxman S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation" // AI Magazine, 38(3). Pp. 50–57. (In English)

Gunning D. (2019). Explainable artificial intelligence (XAI). Defense Advanced Research Projects Agency (DARPA). (In English)

Hajian S., Bonchi F., Castillo C. (2021). Algorithmic bias: From discrimination discovery to fairness-aware data mining // ACM SIGKDD Explorations Newsletter, 21(1). Pp. 14–27. https://doi.org/10.1145/3457309.3457312. (In English)

Hasan M., Chowdhury R., Rahman M. (2022). Smart policing initiatives and AI adoption in Bangladesh // Asian Journal of Law and Technology, 11(2). Pp. 55–74. (In English)

Hossain M., Islam A. (2021). Challenges of data quality in Bangladesh's criminal justice system // International Journal of Criminal Justice, 6(1). Pp. 23–39. (In English)

Human Rights Watch. (2017). China: Police "big data" systems violate privacy, target dissent. (In English)

Human Rights Watch. (2020). China: Police "big data" systems violate privacy, target dissent. https://www.hrw.org/news/2020/01/17/china-police-big-data-systems-violate-privacy. (In English)

Human Rights Watch. (2020). China's use of AI in policing and surveillance. (In English)

Information Commissioner's Office. (2021). Guide to data protection. ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/. (In English)

Joh E. E. (2020). Artificial intelligence and policing: First questions // Annual Review of Law and Social Science, 16. Pp. 359–377. https://doi.org/10.1146/annurev-lawsocsci-101518-042816. (In English)

Kleinberg J., Lakkaraju H., Leskovec J., Ludwig J., Mullainathan S. (2020). Human decisions and machine predictions // The Quarterly Journal of Economics, 133(1). Pp. 237–293. https://doi.org/10.1093/qje/qjz032. (In English)

Kleinberg J., Mullainathan S., Raghavan M. (2018). Inherent trade-offs in the fair determination of risk scores // Proceedings of the 8th Innovations in Theoretical Computer Science Conference. (In English)

Larson J., Mattu S., Kirchner L., Angwin J. (2016). How we analyzed the COMPAS recidivism algorithm. ProPublica. (In English)

*Liang F., Das V., Kostyuk N., Hussain M. M. (*2021). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure // Policy & Internet, 13(4). Pp. 415–453. https://doi.org/10.1002/poi3.259. (In English)

Lum K., Isaac W. (2016). To predict and serve? // Significance, 13(5). Pp. 14–19. (In English)

Mayson S. (2021). Bias in, bias out: Algorithmic fairness and the limits of policy // Yale Law Journal, 130(8). Pp. 2140–2210. https://doi.org/10.2139/ssrn.3478377. (In English)

NACDL. (2020). The Siren song of objectivity: Risk assessment tools and racial disparity. (In English)

ProPublica. (2016). Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks. (In English)

Rahman T. (2021). Corruption, inefficiency, and reforms in Bangladesh criminal justice // Bangladesh Journal of Law, 15(1). Pp. 98–117. (In English)

Raji I. D., Smart A., White R. N., Mitchell M., Gebru T. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing // Proceedings of the Conference on Fairness, Accountability, and Transparency. (In English)

Reuters. (2021, March 30). China found using surveillance firms to help write ethnic-tracking specs. Reuters. https://www.reuters.com/article/us-china-surveillance-idUSKBN2BM1VQ. (In English)

RFA. (2023). In China, AI cameras alert police when a banner is unfurled. (In English)

Richardson R., Schultz J., Crawford K. (2020). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice // New York University Law Review, 94(2). Pp. 192–233. (In English)

Stevenson M., Slobogin C. (2020). Data and discretion: Why we should exercise caution around using the COMPAS algorithm in court. Stanford Rewired. https://law.stanford.edu/publications/data-and-discretion/. (In English)

Talukder K. A., Shompa T. F. (2023). Artificial intelligence in criminal justice management: A systematic literature review // Journal of Machine Learning, Data Engineering and Data Science. (In English)

Tarkey T. (2021). AI-related data ethics oversight in UK policing // Policing: A Journal of Policy and Practice, 15(2). Pp. 790–799. https://doi.org/10.1093/police/paaa061. (In English)

The Guardian. (2025). Predictive policing has prejudice built in. (In English)

The Times. (2025). Pre-crime profiling is no longer a fantasy. (In English)

Trevaskes S., Bernot A. (2023). Surveillance infrastructure in China: Key concepts and mechanisms enhancing the Party-state's governance ambitions // Surveillance & Society. (In English)

Wired. (2024). Judges are using algorithms to justify doing what they already want. (In English)

Zeng W., Li H., Shi Q. (2022). AI surveillance and social credit in China: Implications for criminal justice // Journal of Asian Public Policy, 15(1). Pp. 47–66. (In English)

Zilka M., Fogliato R., Hron J., et al. (2023). The progression of disparities within the criminal justice system: Differential enforcement and risk assessment instruments. arXiv. (In English)

Information about the author

Sohel Rana (Dhaka, Bangladesh) — Candidate of Legal Sciences (PhD in Criminal Law, University of Malaya, Malaysia); LLB (University of London, UK); LLM & LLB (Stamford University Bangladesh); Assistant Professor, Department of Law, University of Information and Technology Sciences (UITS) (e-mail: rana@uits.edu.bd).

Recommended citation

Rana S. AI in criminal justice: a comparative study of predictive policing, risk assessment, and sentencing algorithms. Kazan University Law Review. 2025; 4 (10): 164–189. DOI: 10.30729/2541-8823-2025-10-4-164-189.

Ildar Begishev

Doctor of Legal Sciences, Associate Professor, Chief Researcher, Research Institute of Digital Technologies and Law, Professor, Department of Criminal Law and Process, Kazan Innovative University named after V.G. Timiryasov, Honored Lawyer of the Republic of Tatarstan

Irina Filipova

Candidate of Legal Sciences, Associate Professor, Department of Labour and Environmental Law, Lobachevsky State University of Nizhny Novgorod

PROTECTION OF EMPLOYEES' PERSONAL DATA IN THE CONTEXT OF THE SPREAD OF ALGORITHMIC MANAGEMENT (BASED ON COURT PRACTICE)

DOI: 10.30729/2541-8823-2025-10-4-190-212

Abstract. *The importance of employees' personal data, the protection of which is provided for by current legislation, is changing in the context of the current transformation of labour relations. This is due to the spread of digital technologies, primarily artificial intelligence technologies and products based on them, the efficiency of which directly depends on access to gigantic volumes of data. Employers are increasingly introducing digital technologies into the workplace, which means that the confidentiality of employees' personal data is exposed to additional, previously absent risks, as evidenced by the increasingly extensive case law on this issue. One of the most significant changes made in recent years in the management of production processes is algorithmic management. It is built primarily on the work of artificial intelligence systems that collect numerous data, analyse it, and actually make many decisions for the employer or significantly facilitate their adoption with the intellectual support. Algorithmic management allows for the optimisation of management, including personnel management, but increases the risks of leakage or misuse of information* *required for the operation of artificial intelligence systems, threatening the privacy of employees, which in the long term may become a fairly common cause of labour disputes. A study of existing judicial practice makes it possible to more accurately identify gaps and shortcomings in legal regulation that need to be eliminated, including those that hinder the administration of justice in resolving disputes concerning the processing of employees' personal data by employers.*

Keywords: *personal data, biometrics, employee, right to privacy, employer, algorithmic management, artificial intelligence, labour dispute*

1. Introduction

The question of protecting employees' personal data, access to which employers obtain by virtue of the existence of an employment relationship, has traditionally attracted research interest among labour law specialists[1], who note the vulnerable position of employees and the important role of the developing case law on this issue, which plays a key role in interpreting the law. This topic becomes even more acute owing to the ongoing digitalization and intelligent automation of the sphere of labour, which heightens the risks of violations of employees' rights to privacy (confidentiality) and to the protection of personal data, as noted in their studies by both Russian[2] and foreign legal scholars[3]. Courts are already hearing disputes concerning improper processing by employers of employees' personal data using artificial intelligence, since an employer's deployment of such digital technologies substantially strengthens the employer's position as a party to the employment relationship in comparison with the other party — the employee, who is already the "weaker" party in labour relations. Familiarization with court decisions that have been handed down makes it possible to improve the accuracy of conclusions as to the direction in which the legal regulation of the protection of employees' data will further develop. In rendering decisions on the abovementioned issue, Russian courts rely, first and foremost, on the provisions of two regulatory legal acts — Federal Law No. 152-FZ "On Personal Data" of 27 July 2006 (hereinafter — the Personal Data Law) and the Labour Code of the Russian Federation (Chapter 14). In addition, the position of a specially established executive authority — the Federal Service

[1] *Berezhnov A. A.* (2024). Problemy zashchity personalnykh dannykh rabotnikov na sovremennom etape // Trudovoe pravo v Rossii i za rubezhom = Labor Law in Russia and Abroad, 3. Pp. 8–13.

[2] *Filyushchenko L. I.* (2024). Tsifrovoy profil rabotnika: problemy zashchity personalnykh dannykh // Zakony Rossii: opyt, analiz, praktika = Laws of Russia: experience, analysis, practice, 1. Pp. 28–37.

[3] *Abraha H.* (2023). Regulating algorithmic employment decisions through data protection law // European Labour Law Journal, 14(2). Pp. 172–191. (In English); *De Stefano V.* (2020). "Masters and Servers": Collective Labour Rights and Private Government in the Contemporary World of Work // International Journal of Comparative Labour Law and Industrial Relations, 36(4). Pp. 425–442.

for Supervision in the Sphere of Communications, Information Technologies and Mass Communications (hereinafter — Roskomnadzor) — is also taken into account. Similar legislation exists in foreign jurisdictions as well. The issue under consideration also affects the administration of justice; for example, British researchers note that the online publication of court decisions in employment disputes in the United Kingdom significantly facilitates employers' automated search for the names of job applicants among those listed as claimants, followed by the inclusion of such persons on "blacklists"[1]. As can be seen, problems with the protection of employees' personal data are cross-border in nature and require further study in order to choose a strategy for the future development of legislation and law enforcement in connection with the progressively increasing spread of algorithmic management and artificial intelligence systems (hereinafter — AI systems) in the sphere of labour. This is also confirmed by the discussion of these matters at the level of the International Labour Organization[2].

2. Employees' personal data: concept, composition and significance

Pursuant to the Personal Data Law, personal data includes any information that allows one to identify directly or indirectly a specific natural person, who, in turn, is called the data subject. Personal data is similarly understood by the General Data Protection Regulation (hereinafter — GDPR) of the European Union (hereinafter — EU), to which reference will need to be made repeatedly in the course of comparison, owing to the fact that the said regulatory act is considered the exemplar of regulation in the relevant field, and many of its provisions have been borrowed by regulatory acts subsequently adopted in various countries of the world.

Personal data may be divided into the following groups:

1) general personal data (surname, first name, patronymic, passport data, etc.), section 1 of Article 3 of the Personal Data Law;

2) special data (racial or ethnic origin, political views, religious or philosophical beliefs, health status, intimate life, criminal record), sections 1 and 3 of Article 10 of the Personal Data Law;

3) biometric data—information characterizing physiological features of a human being that allows one to establish his or her identity (photograph, voice, iris, etc.), Article 11 of the Personal Data Law;

4) other data (affiliation to a certain social group, etc.).

An employee's personal data were initially defined by the Labour Code of the Russian Federation as information necessary to the employer in connection with

[1] *Adams Z., Adams-Prassl A., Adams-Prassl J.* (2022). Online tribunal judgments and the limits of open justice // Legal Studies, 42(1). Pp. 42.

[2] *Hendrickx F.* (2022). Protection of workers' personal data: General principles // ILO Working Paper 62. Geneva: ILO. Pp. 5.

the employment relationship and concerning a specific employee, but in 2013 Article 85 of the Labour Code of the Russian Federation, which contained this definition, was repealed. On the basis of the provisions of the Personal Data Law, it is possible to designate as an employee's personal data any information directly or indirectly relating to a specific employee that is processed by an employer within the framework of labour relations.

An employee's personal data may be information included in any of the four groups listed above; it is typically contained in questionnaires completed by employees or job applicants (i.e., persons applying for a job), in employment contracts, in labour books, in payslips, in payroll documents, in photographs of employees, in documents presented by employees upon conclusion of an employment contract, and so on. The law does not provide a closed list of such data. The list of personal data required by the employer is approved by each employer independently and may differ depending on the characteristics of the work and the sphere in which the person works. It should be noted that in Section 10 of the Ruling of the Plenum of the Supreme Court of the Russian Federation of 17 March 2004 No. 2 "On the Application by the Courts of the Russian Federation of the Labour Code of the Russian Federation", emphasis is placed on the absence of any restrictions on employers in choosing a method for assessing the business qualities of a job candidate. "The criteria determining these qualities are not exhaustive, which actually gives employers the right, at their discretion, to use any assessment tools, including systems based on artificial intelligence"[1].

General personal data of an employee may include basic identification data contained in a passport, taxpayer identification number, social insurance number, military records, and may also include:

— employment and biographical information (education, qualifications, work experience, information on previous places of employment and other data from the labour book, position, details of the employment contract, salary—reference to the fact that information about salary is personal data may be found in a letter from Roskomnadzor of 7 February 2014 No. 08KM-3681);

— contact and address data (address of registration and residence, telephone, email address, if the latter can be directly linked to a specific natural person (contains name and surname) or indirectly, when it can be linked to a specific person in the presence of additional information such as a login, and conversely, if an email address is depersonalized, it will not be recognized as personal data; the same applies to telephone numbers);

— information about marital status required by the employer for income tax withholdings.

[1] *Kiyamova D. I.* (2025). Iskusstvennyy intellekt v rekrutinge: zashchita personalnykh dannykh i predotvrashchenie diskriminatsii v tsifrovuyu epokhu // Kadrovik = HR Manager, 5. Pp. 61.

An employee's special data may include:

— health status (information on medical examinations, chronic diseases, disability status);

— trade union membership;

— religious affiliation and nationality.

Biometric data of an employee will be recognized when:

— a photograph is used (for a questionnaire, issuance of a pass, or identification document);

— fingerprints, voice, or facial scan are used (if they are required, in particular, for an access control system).

Other data related to employment activities may include:

— disciplinary penalties;

— materials from official investigations;

— information about access to information systems, etc.

Notwithstanding the recognition of the aforementioned information as personal data as a general rule, in some cases courts refuse to do so. For example, a court refused to recognize as biometric personal data the image of a sleeping employee until such time as it is transmitted for purposes of identification (a decision of the Kineshemsky City Court of Ivanovo Region of 27 May 2021 in case no. 2-873/2021)[1].

Thus, in all the cases under consideration, the data subject is the employee (or the person seeking employment), while the employer is the operator — that is, a legal or natural person that processes the employee's personal data and also determines the purposes of data processing, the composition of personal data to be processed, and the actions (operations) performed with personal data (section 2 of Article 3 of the Personal Data Law). The processing of personal data encompasses not only systematization, clarification, extraction, and depersonalization of data, but also other actions, including: collection, storage, use, transmission, blocking, deletion, and destruction (section 3 of Article 3 of the Personal Data Law).

When speaking of the significance of employees' personal data, it is necessary to recognize that they are an integral element of labour relations (or, if one proceeds from the fact that the elements of any legal relationship are the parties, the object, and the content — a sub-element, a part of the content), which affects the rights of employees and the obligations of employers. Every employer is obliged to obtain and process employees' personal data in compliance with the requirements of the law: to request the employee's consent to data processing as a general rule; to ensure the protection of data from leaks, transmitting it only to state bodies in cases provided

[1] All data on decisions of Russian courts used in the research and referenced in this article were taken from the "Judicial and Normative Acts of the Russian Federation" database (https://sudact.ru/).

for by law; to use the data obtained only for purposes related to employment activity, etc. In addition, since 2022, employers have been required to notify Roskomnadzor of the processing of employees' personal data. Notification must be provided by the data operator before processing begins. In accordance with section 3.1 of Article 22 of the Personal Data Law, with respect to each purpose of data collection, it is necessary to clarify the following parameters: categories of data and data subjects; lists of personal data that will be processed; the legal basis for their processing; a list of actions with personal data and methods of processing. Notification is submitted to the territorial office of Roskomnadzor at the location of the employer in paper form or in electronic form, including through the "State Services" portal. Separate notification must be submitted by the employer within twenty-four hours of the discovery of unlawful or accidental transmission of data (section 3.1 of Article 21 of the Personal Data Law). Special notification is also submitted in the event of cross-border transmission of employees' personal data by the employer. Failure to fulfil these obligations entails administrative liability (Article 19.7 of the Code of Administrative Offences of the Russian Federation).

Employees' personal data have organizational significance for the parties to labour relations. They make it possible to formalize these relations and are necessary for further personnel record-keeping, reporting to state bodies, for example to the tax inspection service. The establishment of a category of personal data guarantees employees the confidentiality of their personal information, grants them the right to control the use of their data, to demand the correction of inaccurate information, and to demand the deletion of information obtained by the employer in violation of law. Thus, employees' personal data are important both for compliance with the law in labour relations (without their use it would be impossible to employ a person) and for the protection of employees' rights (rights to the inviolability of private life), as well as for the safe functioning of the employer (sanctions are provided for data leaks or receipt of data in violation of law). Every employer, except employers who are natural persons not being individual entrepreneurs (Article 22 of the Labour Code of the Russian Federation) and microenterprises (Article 309.2 of the Labour Code of the Russian Federation), is obliged to adopt a Regulation on the Personal Data of Employees. This local regulatory act regulates the organization of work with personal data at a specific employer in accordance with section 8 of Article 86 and Article 88 of the Labour Code of the Russian Federation. The Regulation on Employees' Personal Data should describe the procedure for data processing and list the rights and obligations of the employer and employees. In addition to the aforementioned local regulatory act, the data operator must also publish a policy regarding the processing of personal data, explaining the principles for working with the personal data of employees, customers, and other natural persons (section 2 of section 1 of Article 18.1 of the Personal Data Law).

3. Protection of employees' personal data

An employer must comply with the general principles of personal data processing established by Article 5 of the Personal Data Law. The processing of such data:

1) must be carried out on a lawful and fair basis and must be limited to achieving specific, predetermined, and lawful purposes;

2) does not permit the combination of databases containing personal data whose processing is carried out for purposes that are incompatible with each other;

3) must encompass only data that meets the purposes of processing, without excess;

4) must ensure the accuracy of personal data, their sufficiency, and, where necessary, their relevance with respect to the purposes of processing;

5) requires the destruction or depersonalization of data upon achievement of the purposes of processing or in the event of loss of the need to achieve such purposes, unless otherwise provided by federal law.

6) Furthermore, from 1 July 2025 onwards, Russia prohibits the processing of personal data through foreign services (section 5 of Article 18 of the Personal Data Law).

Requirements for the processing of employees' personal data directly are set out in Article 86 of the Labour Code of the Russian Federation:

— processing may be carried out exclusively for the purposes of compliance with the law, assistance to employees in finding employment, obtaining education and promotion, ensuring the personal safety of employees, monitoring the work performed, and preserving property (special attention should be paid to the last two items, which are aimed at protecting the interests of the employer);

— in determining the scope and content of an employee's processed data, the employer must be guided by the law;

— all personal data of an employee should be obtained from the employee himself or with the written consent of the employee;

— an employer does not have the right to obtain and process personal data belonging to the category of special data, except in cases provided for by law (for example, an employer has the right to process information about an employee's health status that is relevant to the employee's ability to perform his or her labour function, in accordance with Article 69 of the Labour Code of the Russian Federation; for this, the employer does not even need to obtain the consent of the employee);

— an employer does not have the right to request information about an employee's membership in public associations, including trade unions, again, except in cases provided for by law;

— in making decisions affecting an employee's interests, an employer does not have the right to rely on personal data obtained exclusively as a result of automated processing or electronic receipt (without human participation);

— protection of an employee's personal data from unlawful use or loss must be ensured by the employer in the manner provided for by law at the employer's own expense;

— employees and their representatives must be informed by signature of the employer's documents establishing the procedure for processing personal data, with information about their rights and obligations in this area;

— there is no provision for employees' refusal of their rights to preserve and protect confidentiality;

— employers, employees, and their representatives should jointly develop measures to protect employees' personal data.

The aforementioned principles and requirements for the processing of personal data form the basis of a legislative-restrictive approach to the protection of employees' personal data. Within the framework of the existing approach, an employer must obtain an employee's consent to the processing of his or her personal data as a general rule (except, for example, for the legally required transmission of data to state bodies — the Social Fund of Russia, military commissariat, tax inspectorate, etc.). Consent may be included in the employment contract or may be executed as a separate document, and the employee may later withdraw his or her consent. In the latter case, the employer will be able to continue processing personal data in the minimum scope necessary to preserve labour relations (section 5 of section 1 of Article 6 of the Personal Data Law). Upon withdrawal of consent, it will not be possible, for example, to process biometric data of the employee. Some data the employer will not be able to delete even after the dismissal of the person who has withdrawn consent, in compliance with the requirements of Federal Law of 22 October 2004 No. 125-FZ "On Archival Work in the Russian Federation", in accordance with which a number of documents on personnel must be stored for up to 75 years. It should be noted that the dissemination of an employee's personal data requires separate written consent (Article 10.1 of the Personal Data Law).

Upon discovery of violations, the employer will be held liable in the form of a fine. Notwithstanding the fact that an employer who has disregarded the established procedure for processing personal data is held administratively liable, claims for the protection of personal data are considered in accordance with the rules of civil procedure, as follows from section 6.1 of Article 29 of the Code of Civil Procedure of the Russian Federation. This also applies to situations where, in the interests of a specific citizen, a claim for the protection of his or her rights as a data subject is brought by Roskomnadzor, which has the right to apply to the court with a statement in protection of the rights, freedoms, and legitimate interests at the request of a specific person or in protection of the rights, freedoms, and legitimate interests of an indefinite circle of persons on the basis of Article 46 of the Code of Civil Procedure of the Russian Federation (a ruling of the Civil Chamber of the Supreme Court of the Russian Federation of 14 July 2020 No. 58-КГ20-2). In addition, civil law liability of the employer is provided for — compensation of losses (Article 15 of the Civil Code of the Russian Federation) and compensation for non-pecuniary damage (Article 151 of the Civil Code of the Russian Federation). Employees directly responsible for the violation may be held liable to disciplinary or even criminal responsibility.

The general principles and requirements for the processing of personal data are reflected in court decisions concerning the protection of employees' personal data. Thus, courts strictly assess the correspondence of the information requested to the purposes of processing. An employer may request only necessary data; if it demands the provision of excessive information, it violates the employee's right to the inviolability of private life and the right to the protection of personal data. Typical violations by employers of the procedure for processing personal data include: absence of the employee's consent to data processing (in cases where it is required); use of data for personal purposes not related to the employee's employment activity; transmission of data to third parties without sufficient grounds.

As practice shows, currently a significant portion of labour disputes are related to the use of video surveillance in the process of work. Courts, in considering such disputes, ascertain the lawfulness of the implementation of video surveillance, which will be considered lawful if:

— the use of video surveillance is mentioned in the Rules of Internal Labour Procedure, or the employer has adopted a separate local regulatory act — a Regulation on Video Surveillance, with which employees are acquainted by signature;

— there is the employee's consent to the processing of personal data, including the processing of data obtained in the course of video surveillance;

— video cameras are installed only at work stations, in production premises, in corridors, but not in changing rooms, rest rooms, toilets, and shower rooms;

— employees are notified of the surveillance and of the visibility zones of the cameras;

— recordings are not posted on the internet and are not transmitted to third parties.

In accordance with Article 22 of the Labour Code of the Russian Federation, an employer has the right to require employees to perform their employment duties, to comply with labour discipline, and to treat the employer's property with care. "The law does not specify exactly how an employer may monitor subordinates, therefore, the establishment of video surveillance to achieve a purpose related to the labour process is not a measure contrary to the law" (a decision of the Hostinsky District

Court of Sochi of 13 January 2025 in case no. 2-4578/2024). Permissible purposes of video surveillance include: monitoring the efficiency of work, improving labour productivity, control and accounting of working hours. If an employee has not given consent to the processing of biometric personal data, this does not mean that the employer does not have the right to conduct video surveillance. Such surveillance is possible if all employees have been acquainted by signature with the local regulatory act mentioning video surveillance (if an employee does not agree to sign a statement of acquaintance, an appropriate act is drawn up), and in premises where there are video cameras, warning notices are displayed indicating the openness of the surveillance. Accordingly, video surveillance in premises intended for employee rest is not permitted, as it violates the employee's right to the inviolability of private life (a ruling of the Third Cassation Court of General Jurisdiction of 3 July 2023 in case no. 88-14171/2023).

With the development of digital technologies, the use of employees' biometric data is becoming increasingly common. It should be noted that the processing of biometrics includes the use by an employer of an employee's photograph, including for image-related purposes. The fact of an employee's participation in a photo shoot does not mean consent to the use of the image by the employer; written consent of the employee is required (a ruling of the Second Cassation Court of General Jurisdiction of 4 July 2023 in case no. 88-13675/2023).

The number of labour disputes related to employers' making of decisions exclusively on the basis of automated data processing or electronic receipt of data is also increasing, which is not permitted under section 6 of Article 86 of the Labour Code of the Russian Federation. Thus, in a decision of the Balashikha City Court of Moscow Region of 14 January 2025 in case no. 2-11858/2024, it is emphasized that the law prohibits subjecting employees to disciplinary liability solely on the basis of information obtained from the functioning of an electronic access control system. Employees' applications to court may concern information leaks due to insufficient protection of data by the employer, disclosure of personal data, or refusal to provide an employee access to his or her personal data. Usually, in such cases, plaintiffs, in addition to restoration of the violated right, demand compensation for non-pecuniary damage. A typical example of courts' decisions on such questions is the decision of the Sverdlov District Court of Kostroma of 24 December 2024 in case no. 2-4521/2024, which recognizes the employer's inaction (failure to provide information requested by the employee regarding the processing of his or her personal data) as unlawful and grants the employee's claim for compensation for non-pecuniary damage.

A separate question deserves attention: does an employer have the right to disseminate information about disciplining a specific employee? Discussion of this question reached the Constitutional Court of the Russian Federation. The claimant challenged the constitutionality of section 1 of Article 152 of the Civil Code of the Russian Federation, according to which a person has the right to demand the refutation of information damaging his or her honour, dignity, or business reputation only if the person who disseminated the information does not prove that it is true. By a Ruling of the Constitutional Court of the Russian Federation of 21 July 2023 No. 44-П "In the Case Concerning a Check of the Constitutionality of Section 1 of Article 152 of the Civil Code of the Russian Federation in Connection with a Complaint of Citizen E.A. Popkova", the aforementioned section of Article 152 of the Civil Code of the Russian Federation was recognized as corresponding to the Constitution of the Russian Federation, as a result of which the employer's right to determine the expediency of disseminating information about an employee subjected to disciplinary punishment, provided that the information corresponds to the purposes of its dissemination, was confirmed.

4. The impact of algorithmic management on the sphere of labour and employee rights

Algorithmic management (algorithmic governance)[1] is the automated management of employees and business processes within an organization for purposes of optimization. Automation of management entails the making of decisions on the basis of the use of AI systems, which increasingly actually perform the employer's functions in fact, from the hiring of workers to their dismissal.

Algorithmic management includes:

1) automated data collection and monitoring of employees;
2) real-time response to data used for making management decisions;
3) automated or semi-automated decision-making;
4) conversion of performance assessments into rating systems and other metrics;
5) the use of "nudging" to indirectly encourage particular employee behaviour[2].

Initially, algorithmic management penetrated the sphere of labour through digital labour platforms; gradually, new digital tools came to be applied by "traditional" employers as well. The EU Regulation on Artificial Intelligence, adopted in 2024[3],

[1] Algorithmic management as algorithmic control at the micro level, should be distinguished from the concept of Algorithmic governance, that is, algorithmic management at the macro level through the use of algorithms to regulate and coordinate social, economic, and political processes in society, including state and corporate governance.

[2] *Filipova I. A.* (2023). Algoritmicheskiy menedzhment i tsifrovoe profilirovanie v sfere truda // Trudovoe pravo v Rossii i za rubezhom = Labor Law in Russia and Abroad, 1. Pp. 16.

[3] 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) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (date of address: 10.08.2025).

confirms that automated decision-making in the workplace entails significant risks to decent working conditions and the protection of workers' rights (AI systems applied in the field of employment and personnel management are classified as high-risk). The subsequent adoption of the EU Directive on improving working conditions on digital labour platforms[1] was aimed at increasing the level of transparency in the application of artificial intelligence for the functioning of digital platforms. Thus, the task of preserving human control over compliance with working conditions was accomplished, and workers were given the right to challenge automated decisions. This directive, according to European legal scholars, was a step forward for European legislation, but since it concerns only digital labour platforms, it has not satisfied the growing need to regulate the application of algorithmic management in the sphere of labour as a whole. Regulation of such application will require the adoption of another legal act — a Directive on Algorithmic Management, a draft of which has already been created and includes a prohibition on particularly harmful practices, the right to challenge automated decision-making in "traditional" workplaces, and so on[2]. For the use of digital tools by any employer enables large-scale monitoring and data collection, leading to violations of confidentiality, reducing the level of protection of workplaces and worker autonomy[3].

Algorithmic management is carried out on the basis of various systems that automate management processes, including:

— project planning and management systems that carry out real-time monitoring, analysis of data obtained with the identification of trends, forecasting of probable future events, distribution of tasks, resources, and control of deadlines;

— human resource management systems that optimize personnel work through data analysis, enabling improved management of work performance and worker engagement;

— AI recruiters — digital platforms for personnel selection that accelerate the search for the most suitable candidates for jobs whilst simultaneously reducing the costs of such search[4];

[1] Directive (EU) 2024/2831 of the European Parliament and of the Council of 23 October 2024 on improving working conditions in platform work. Available: URL: https://eur-lex.europa.eu/eli/dir/2024/2831/oj (date of address: 10.08.2025).

[2] *Adams-Prassl J., Abraha H., Kelly-Lyth A., Silberman M., Rakshita S.* (2023). Regulating algorithmic management: A blueprint // European Labour Law Journal, 14(2). Pp. 124.

[3] *Cox Th., Oosterwijk G. R.* (2024). Algorithmic management in traditional workplaces. Case studies on the impact of algorithmic technologies in seven sectors in the Nordics // Policy Study. Brussels: FEPS. Pp. 3.

[4] *Lipko V. D., Lipko N. I.* (2025). Tsifrovaya transformatsiya kadrovykh protsessov v epokhu tekhnologiy // Kadrovik = HR Manager, 6. Pp. 56.

— decision support systems that generate recommendations, providing intellectual assistance in analysis, forecasting, and choice of solutions in complex situations.

Next, we shall identify the main consequences of the implementation of algorithmic management by employers, which create or exacerbate already existing problems.

Consequence 1. The implementation of algorithmic management creates a need for large volumes of data for the proper functioning of AI systems. Obtaining such data is possible by means of access to numerous databases and the use of a variety of sensors. AI monitoring has become standard practice, "based on advanced computational methods to obtain statistical inferences about workers on the basis of their data. These inferences are subsequently used by employers to make various organizational and management decisions", which effectively turns workers into "data-based commodities… the boundaries between technological innovation and human individuality are becoming increasingly blurred, challenging traditional understandings of confidentiality"[1].

A worker risks finding themselves "behind glass"; their private life becomes a fiction. The problem of reduced confidentiality is intensified by the spread of wearable devices used in healthcare to help diagnose diseases and monitor an individual's health status. Some of these devices have already been brought to market and are used in the workplace for purposes of protecting workers' health and safety. Neither Russian nor European legislation yet regulates the use of wearable devices in the sphere of labour, which increases the problem of realizing the worker's right to the inviolability of their private life. The existing regulatory framework relates to the use of medical devices and is focused on the safety, performance, and quality of technological products, but is unable to address data protection problems associated with the use of wearable devices for purposes of occupational health and safety[2]. Discrepancies between labour legislation and occupational health and safety legislation leave room for the use of various high-technology systems to collect information about the worker and their participation in the production process[3].

Consequence 2. The use of algorithmic management makes it possible not only to collect but also to generate vast volumes of new information about

[1] *Carter C.* (2025). AI surveillance: Reclaiming privacy through informational control // European Labour Law Journal, 16(2). Pp. 245.

[2] *Marassi S., Földes M.É.* (2025). From healthcare to employment: Tackling the regulatory challenges of in-body wearable devices at work in the European Union // European Labour Law Journal, 16(2). Pp. 195.

[3] *Zaitseva L.V.* (2024). Risks for Personal Data of an Employee When the Employer Uses Technologies of Artificial Intelligence in the Countries of the Eurasian Economic Union // European and Asian Law Review, 7(4). Pp. 31.

workers, each of whose actions leaves a digital trace. This trace can be recorded and analyzed using artificial intelligence with minimal effort and cost. Digital traces and the results of their intelligent processing fill the created digital profile of each worker as a collection of current and reliable data about a specific person in digital format. The employer (through AI systems functioning to achieve the goals set by the employer) gains access to data that makes it possible to make management decisions optimal for the employer on the basis of information about the worker, of which the worker himself or herself may not yet even be aware. This is facilitated by the use of personnel electronic document circulation, the maintenance of which is permitted by Articles 22.1–22.3 of the Labour Code of the Russian Federation.

Already at the stage of employment, intelligent analysis of data obtained from the job applicant and from external sources makes it possible to identify hidden risks associated with the candidate and to prevent him or her from passing through the "entry" filter[1]. Thus, algorithmic management increases the risk of discrimination against job candidates, while simultaneously threatening the inviolability of their private life. Moreover, discrimination is the easiest to detect from a technical point of view. As a result, thanks to the employer's access to technical information about the operation of AI systems (through the specialists he or she has) and the absence of comparable access for the job seeker, the problem of discrimination will be exacerbated. The same applies not only at the stage of employment but also in subsequent periods of work, since although "the automation of decision-making processes previously performed by humans may make the criteria for discrimination more traceable and the results more quantitative… algorithmic decision-making processes are rarely transparent"[2].

Consequence 3. Algorithmic management is an element of intelligent automation of production, the degree of which is continuously increasing. In a number of sectors, there is already an "expulsion" of some workers from their jobs, with reference being made to call centres, the banking sector, and logistics. Other workers are forced to come to terms with the fact that their rights, enshrined in legislation formed predominantly under the conditions of Society 3.0 (industrial society), are meaning less and less in practice under the current stage of civilization's development — Society 4.0 (post-industrial information society) — and risk becoming meaningless formalities in the era of the merger of physical and digital environments — the future of Society 5.0 (Smart Society). Thus, a problem emerges of ensuring real guarantees of workers' rights in the conditions of a society managed with the aid

[1] *Filipova I. A.* (2023). Algoritmicheskiy menedzhment i tsifrovoe profilirovanie v sfere truda // Trudovoe pravo v Rossii i za rubezhom = Labor Law in Russia and Abroad, 1. Pp. 17.

[2] *Kelly-Lyth A.* (2023). Algorithmic discrimination at work // European Labour Law Journal, 14(2). Pp. 152.

of artificial intelligence, the approach of which is signalled, among other things, by the spread of algorithmic management.

For now, case law on the use of algorithmic management is largely related to work based on digital platforms, which corresponds to the chronology of the spread of algorithmic management in the sphere of labour. This is illustrated by numerous decisions of American and European courts handed down in claims by taxi drivers and couriers, as well as decisions of Russian courts, in particular concerning the services "Yandex.Taxi" and "Yandex.Food", for example, a decision of the Peace Court of the Zamoskvoretsky District of Moscow of 2 August 2022 imposing a fine for the leakage of personal data of "Yandex.Food" couriers. Indeed, algorithmic management increases the threat of data leaks, as the employer's information systems contain numerous information about workers, the disclosure of which may result from cyber-attacks on these systems or unlawful access by insiders. Additionally, risks related to the use of cloud services and mobile devices for processing and storing personal information are increased[1]. In addition, personal data are often used as training data in the training of AI models or the "retraining" of AI systems, the results of which depend on the set of databases "feeding" these systems[2]. An additional risk is the connection to "open" AI systems, including chatbots, since information entered into such an AI system may be unintentionally transmitted to another user and retained for use in further training of that AI system[3].

5. Ways of solving problems related to the spread of algorithmic management

At the present time, the transformation of labour relations and the sphere of labour as a whole continues, which has become an inevitable consequence of society's transition from an industrial to a post-industrial type[4], and moreover, the prospects for a further transformation are already emerging, related to humanity's forthcoming transition to Society 5.0, in which digital technologies will occupy an even more important place. The rising intelligent automation of production as a sustained trend is supplemented by the spread of algorithmic management:

[1] *Novikov P. A.* (2025). Sovremennye vyzovy v obespechenii zashchity personalnykh dannykh rabotnikov // Yuridicheskie issledovaniya = Legal Studies, 3. Pp. 29.

[2] *Lukács A., Váradi S.* (2023). GDPR-compliant AI-based automated decision-making in the world of work // Computer Law & Security Review, 50. Art. 105848.

[3] *Novikov D. A.* (2024). Ispolzovanie iskusstvennogo intellekta pri naime rabotnikov: problemy i perspektivy pravovogo regulirovaniya // Journal of Digital Technologies and Law, 2(3). Pp. 616.

[4] *Tomashevskiy K. L.* (2025). Transformatsiya trudovykh pravootnosheniy (ot industrialnogo k postindustrialnomu tipu) // Zhurnal rossiyskogo prava = Journal of Russian Law, 29(2). Pp. 94.

AI systems increasingly not only take positions alongside workers but also manage production processes. From the perspective of the employer, such a "digital future" obviously has a positive effect, as it leads to reduced costs, increased productivity, and the possibility, when making decisions, of relying on volumes of data that human beings would simply be unable to process. At the same time, as social researchers warn, the application of algorithmic management potentially creates an imbalance between the technical and social subsystems of an organization, a vivid example of which is the company Amazon.

Workers typically act as a passive object of the implementation of new technologies[1], so the main efforts are directed at adapting the social subsystem to the requirements of the technical subsystem, including minimizing worker resistance, rather than using technologies from the outset with consideration for the specifics of the work[2]. Self-learning AI systems are capable of adapting to new situations, making it possible to delegate to them the making of an increasingly broad range of decisions. Such self-learning is typically opaque, leaving no opportunity to identify the reasons for subsequent decisions and to challenge them[3].

A dilemma emerges: parallel to the increasing transparency of workers to AI systems (through the processing of growing volumes of their personal data), the degree of opacity of decision-making for workers increases due to the use of algorithmic management. It is difficult to combat trends, but at least it is possible to adjust them. One of the solutions capable of preventing the degradation of workers' position is a prohibition enshrined in legislation on making decisions exclusively on the basis of automated data processing (section 6 of Article 86 of the Labour Code of the Russian Federation, section "h" of Article 15 of the GDPR).

As is well known, the EU aspires to global leadership in the formulation of legislation taking into account the development of digital technologies, but even in the provisions of the GDPR relating to automated decision-making and providing workers with certain protection, serious gaps remain. For example, most management decisions today are made with the aid of algorithms, but not fully automated, and in such cases the guarantees provided for in Article 22 of the GDPR (including the right to challenge a decision) are not applicable[4]. At the same time, the results of research

[1] *Parker S. K., Grote G.* (2020). Automation, algorithms, and beyond: Why work design matters more than ever in a digital world // Applied Psychology, 71(4). Pp. 1171.

[2] *Davis M. C., Challenger R., Jayewardene D. N., Clegg C. W.* (2014). Advancing socio-technical systems thinking: A call for bravery // Applied ergonomics, 45(2). Pp. 171.

[3] *Petrovskaya I. A., Demchenko V. S.* (2023). Algoritmicheskiy menedzhment: opyt empiricheskogo issledovaniya // Vestnik Moskovskogo universiteta. Seriya 6. Ekonomika = Moscow University Economics Bulletin, 58(6). Pp. 129.

[4] *Abraha H.* (2023). Regulating algorithmic employment decisions through data protection law // European Labour Law Journal, 14(2). Pp. 172–191.

in the field of economics show that algorithmic management "is likely to become a notable component of work for many people in the coming years"[1].

The increasing technical possibilities for monitoring workers require legislative limitations not only on the control of the employee's performance of labour duties but also on the process of using the data obtained to make personnel decisions. It becomes necessary to consider the employee's right to the inviolability of private life as one of the fundamental principles of the legal regulation of labour relations[2] with appropriate reflection in the law.

In connection with "the unprecedented scale, depth, rapid pace of transformation, and pervasive impact on labour" of algorithmic management, a draft Directive on Algorithmic Management in the Workplace[3] was submitted for discussion in the European Parliament in 2025 (hereinafter — the draft Directive). In the opinion of representatives of the Committee on Employment and Social Affairs of the European Parliament, who are the authors of the draft, the prohibition provided for in the GDPR on fully automated decision-making in a number of cases, for example in hiring, is insufficient. After approval, the new regulatory act should establish a common EU standard for the use of algorithmic management in the workplace, ensuring enhanced transparency and legal certainty in all EU Member States.

According to Article 3 of the draft Directive, no later than the first working day (or immediately before any change in the employment contract, as well as at any time upon receipt of a request from the employee), the employer, in clear and comprehensible form, without unnecessary technical complexity, must provide the employee in writing with information relating to the use or planned use of algorithmic management. The information is necessary for understanding how algorithmic systems will affect decisions affecting workers. This information will include the categories of collected and processed data and the types of worker actions tracked. In accordance with Article 5 of the draft Directive, as a guarantee of workers' rights, processing of personal data concerning the emotional state of workers, neuro-surveillance, private conversations, worker behaviour outside working hours, as well as predictions regarding the realization of workers' fundamental rights and conclusions about racial or ethnic origin, migration status, political views, religious

[1] *De Stefano V.* (2022). AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU's Legal Framework // Brussels: European Parliamentary Research Service. Pp. 7.

[2] *Serova A. V., Shcherbakova O. V.* (2022). The Employee's Right to Privacy Transformation: Digitalization Challenges // Kutafin Law Review, 9(3). Pp. 437.

[3] Draft report with recommendations to the Commission on digitalisation, artificial intelligence and algorithmic management in the workplace — shaping the future of work (2025/2080(INL)), 26.06.2025. URL: https://www.europarl.europa.eu/doceo/document/EMPL-PR-774283_EN.pdf (date of address: 10.08.2025)

beliefs, health status, trade union membership, or sexual orientation should be directly included in prohibited practices.

Article 6 of the draft Directive refers to the need to maintain human control so that an interested worker is able to obtain from the employer an explanation regarding any decision affecting various aspects of labour relations with him or her. These aspects include distribution of tasks, assessment of labour productivity, working hours schedule, pay, disciplinary penalties, and so on, if the making of the decision was substantially influenced by an algorithmic system. Decisions, however, concerning the beginning or termination of labour relations, any changes in pay cannot in principle be made exclusively on the basis of algorithmic management, but must be considered and finally rendered by a human manager.

The rules proposed by the draft Directive will make it possible to change the new management structure to a more humane one, since algorithmic management is an innovation that changes the relationship between humans and artificial intelligence in the production environment, and in the absence of sufficient control, as M. A. Yudina aptly stated, "may become the last nail in the coffin of confidentiality in the reality of social networks, smart homes, smart cities, and electronic government"[1].

Of course, in the processing of personal data, the principle of lawfulness must be observed first and foremost. If one refers to the practice of the European Court, one may be assured that processing of personal data will be considered lawful with the mandatory observance of the following three conditions:

— processing must correspond to the purpose of pursuing legitimate interests;

— processing must be necessary to achieve such purposes;

— legitimate interests must not override the interests or fundamental rights and freedoms of the data subject.

This is about a phased assessment of proportionality: sufficiency for achieving a legitimate purpose, necessity for achieving that purpose, and balance between achieving the purpose and the rights of the data subject[2]. At the same time, the European Court clarified that the necessity of processing should be assessed taking into account the principle of data minimization set out in section "c" of Article 5 of the GDPR[3]. Legitimate interests of the employer, if they are insignificant

[1] *Yudina M. A.* (2024). Algorithmic management in the focus of sociology of technology // RUDN Journal of Sociology, 24(3). Pp. 744.

[2] *Dalla Corte L.* (2022). On proportionality in the data protection jurisprudence of the CJEU // International Data Privacy Law, 12(4). Pp. 264.

[3] Judgment of the Court (Grand Chamber) of 4 July 2023. Meta Platforms Inc and Others v Bundeskartellamt. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252 (date of address: 10.08.2025).

and not too compelling, may override the interests and rights of workers only in those cases where the impact on those rights and interests is even more insignificant[1].

The aforementioned tasks will have to be solved by the Russian legislator as well, supplementing and amending labour legislation. Here an important point becomes the inclusion of the definition of the very concept of "employees' personal data" in the Labour Code of the Russian Federation. Whereas prior to 2013, an employee's personal data were defined in Article 85 of the Labour Code of the Russian Federation as information necessary to the employer in connection with the employment relationship and concerning a specific employee, in 2013 Article 85 of the Labour Code of the Russian Federation was repealed. As a result, Chapter 14 of the Labour Code of the Russian Federation was "decapitated", leaving only the articles following Article 85 of the Labour Code of the Russian Federation, devoted to individual issues of the processing of personal data, thereby complicating the task for the legal practitioner in understanding and interpreting the law. The return (more precisely, the inclusion in the Labour Code of the Russian Federation of an updated, more comprehensive formulation) of this concept is needed by judges considering relevant cases. Confirmation of this may be provided by the fact that in decisions rendered by Russian courts, references to Article 85 of the Labour Code of the Russian Federation are still encountered. Examples include a decision of the Vakhitovsky District Court of Kazan of 25 February 2025 in case no. 2-1947/2025, a decision of the Georgievsky City Court of Stavropol Territory of 24 February 2025 in case no. 2-293/2025, a decision of the Lenin District Court of Tyumen of 3 September 2024 in case no. 2-7749/2024, and several others. An updated legal definition of employees' personal data should take into account the growing use of algorithmic management in the production environment. As a possible variant, we propose to formulate the content of Article 85 of the Labour Code of the Russian Federation as follows:

"Employees' personal data are any information relating to a directly or indirectly identified or identifiable natural person (employee) that is processed by an employer within the framework of labour relations, including data collected in the process of algorithmic management (biometric data, digital traces, behavioural metrics, and derived data as results of automated analysis generated by algorithms)".

The return of an updated definition of employees' personal data directly to the labour legislation of the Russian Federation will contribute to the improvement of legal regulation in this area and will have a positive impact on law enforcement.

[1] *Warter J.* (2025). The legitimacy of modern data processing in the workplace // European Labour Law Journal, 16(2). Pp. 180–181.

Conclusion

In the dawning era of artificial intelligence, already having acquired the steady designation in the English-language variant of "AI-driven world", human personal data are "fuel" for AI systems, enabling them to learn and function with increasing levels of effectiveness. Entrepreneurs acting as employers find in AI systems very useful intellectual helpers that optimize production and management processes. The further things go, the more digital technologies prevail over the social environment, transforming it and subjecting it to new rules. Employees' personal data become more vulnerable with each passing year, and the implementation by employers of algorithmic management in the workplace only intensifies this trend. Workers risk finding themselves "under glass" with the gradual transformation of confidentiality into fiction. Particular attention is required to the now technically accessible acquisition of biometric data by employers, since intelligent analysis of such data makes it possible to forecast probable human behavior and health status in the future. Legal regulation in the field of personal data protection lags behind technological achievements in terms of speed of formation. The problems caused by this are linked, first and foremost, to the reduction of confidentiality, but also to the increase in the risk of discrimination and, accordingly, to the provision of real guarantees of workers' rights in the conditions of the development of a society managed with the aid of artificial intelligence. The aforementioned problems are readily "readable" when one refers to case law, both Russian and foreign. The solution of these problems lies not only in the legislative sphere but also in the sphere of law enforcement. In order for justice to perform its task most effectively, the court must rely on a quality legislative base. Consequently, the elimination of gaps in the legislation regulating the protection of employees' personal data, in particular in the Labour Code of the Russian Federation, will help to ensure this protection, minimizing the risks that emerge or increase owing to the spread of algorithmic management and the rising intelligent automation of the sphere of labour.

References

Abraha H. (2023). Regulating algorithmic employment decisions through data protection law // European Labour Law Journal, 14(2). Pp. 172–191. (In English)

Adams-Prassl J., Abraha H., Kelly-Lyth A., Silberman M., Rakshita S. (2023). Regulating algorithmic management: A blueprint // European Labour Law Journal, 14(2). Pp. 124–151. (In English)

Adams Z., Adams-Prassl A., Adams-Prassl J. (2022). Online tribunal judgments and the limits of open justice // Legal Studies, 42(1). Pp. 42–60. (In English)

Berezhnov A. A. (2024). Problemy zashchity personalnykh dannykh rabotnikov na sovremennom etape // Trudovoe pravo v Rossii i za rubezhom = Labor Law in Russia and Abroad, 3. Pp. 25–28. (In Russian)

Carter C. (2025). AI surveillance: Reclaiming privacy through informational control // European Labour Law Journal, 16(2). Pp. 245–258. (In English)

Cox Th., Oosterwijk G. R. (2024). Algorithmic management in traditional workplaces. Case studies on the impact of algorithmic technologies in seven sectors in the Nordics // Policy Study. Brussels: FEPS. 60 p. (In English)

Dalla Corte L. (2022). On proportionality in the data protection jurisprudence of the CJEU // International Data Privacy Law, 12(4). Pp. 259–275. (In English)

Davis M. C., Challenger R., Jayewardene D. N., Clegg C. W. (2014). Advancing socio-technical systems thinking: A call for bravery // Applied ergonomics, 45(2). Pp. 171–180. (In English)

De Stefano V. (2022). AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU's Legal Framework // Brussels: European Parliamentary Research Service. 84 p. (In English)

De Stefano V. (2020). "Masters and Servers": Collective Labour Rights and Private Government in the Contemporary World of Work // International Journal of Comparative Labour Law and Industrial Relations, 36(4). Pp. 425–442. (In English)

Filipova I. A. (2023). Algoritmicheskiy menedzhment i tsifrovoe profilirovanie v sfere truda // Trudovoe pravo v Rossii i za rubezhom = Labor Law in Russia and Abroad, 1. Pp. 16–18. (In Russian)

Filyushchenko L. I. (2024). Tsifrovoy profil rabotnika: problemy zashchity personalnykh dannykh // Zakony Rossii: opyt, analiz, praktika = Laws of Russia: experience, analysis, practice, 1. Pp. 93–97. (In Russian)

Hendrickx F. (2022). Protection of workers' personal data: General principles // ILO Working Paper 62. Geneva: ILO. 55 p. (In English)

Kelly-Lyth A. (2023). Algorithmic discrimination at work // European Labour Law Journal, 14(2). Pp. 152–171. (In English)

Kiyamova D. I. (2025). Iskusstvennyy intellekt v rekrutinge: zashchita personalnykh dannykh i predotvrashchenie diskriminatsii v tsifrovuyu epokhu // Kadrovik = HR Manager, 5. Pp. 59–67. (In Russian)

Lipko V. D., Lipko N. I. (2025). Tsifrovaya transformatsiya kadrovykh protsessov v epokhu tekhnologiy // Kadrovik = HR Manager, 6. Pp. 56–60. (In Russian)

Lukács A., Váradi S. (2023). GDPR-compliant AI-based automated decision-making in the world of work // Computer Law & Security Review, 50. Art. 105848. (In English)

Lushnikov A. M. (2022). Tsifrovizatsiya trudovogo prava i trudovye otnosheniya // Zakon = Law, 10. Pp. 28–37. (In Russian)

Marassi S., Földes M.É. (2025). From healthcare to employment: Tackling the regulatory challenges of in-body wearable devices at work in the European Union // European Labour Law Journal, 16(2). Pp. 195–211. (In English)

Novikov D.A. (2024). Ispolzovanie iskusstvennogo intellekta pri naime rabotnikov: problemy i perspektivy pravovogo regulirovaniya // Journal of Digital Technologies and Law, 2(3). Pp. 611–635. (In Russian)

Novikov P.A. (2025). Sovremennye vyzovy v obespechenii zashchity personalnykh dannykh rabotnikov // Yuridicheskie issledovaniya = Legal Studies, 3. Pp. 28–44. (In Russian)

Parker S.K., Grote G. (2020). Automation, algorithms, and beyond: Why work design matters more than ever in a digital world // Applied Psychology, 71(4). Pp. 1171–1204. (In English)

Sapfirova A.A. (2024). Pravovye mery obespecheniya bezopasnosti personalnykh dannykh rabotnikov pri ikh obrabotke rabotodatelyami // Kadrovik = HR Manager, 12. Pp. 8–13. (In Russian)

Serova A.V., Shcherbakova O.V. (2022). The Employee's Right to Privacy Transformation: Digitalization Challenges // Kutafin Law Review, 9(3). Pp. 437–465. (In English)

Petrovskaya I.A., Demchenko V.S. (2023). Algoritmicheskiy menedzhment: opyt empiricheskogo issledovaniya // Vestnik Moskovskogo universiteta. Seriya 6. Ekonomika = Moscow University Economics Bulletin, 58(6). Pp. 109–132. (In Russian)

Tomashevskiy K.L. (2025). Transformatsiya trudovykh pravootnosheniy (ot industrialnogo k postindustrialnomu tipu) // Zhurnal rossiyskogo prava = Journal of Russian Law, 29(2). Pp. 94–109. (In Russian)

Warter J. (2025). The legitimacy of modern data processing in the workplace // European Labour Law Journal, 16(2). Pp. 179–194. (In English)

Yudina M.A. (2024). Algorithmic management in the focus of sociology of technology // RUDN Journal of Sociology, 24(3). Pp. 734–746. (In English)

Zaitseva L.V. (2024). Risks for Personal Data of an Employee When the Employer Uses Technologies of Artificial Intelligence in the Countries of the Eurasian Economic Union // European and Asian Law Review, 7(4). Pp. 22–34. (In English)

Information about the authors

Ildar Begishev (Kazan, Russia) — Doctor of Legal Sciences, Associate Professor, Chief Researcher, Research Institute of Digital Technologies and Law, Professor, Department of Criminal Law and Process, Kazan Innovative University named after V.G. Timiryasov, Honored Lawyer of the Republic of Tatarstan (42 Moskovskaia St., Kazan, 420111, Russia; e-mail: begishev@mail.ru).

Irina Filipova (Nizhny Novgorod, Russia) — Candidate of Law, Associate Professor, Associate Professor of the Department of Labor and Environmental Law, National Research Nizhny Novgorod State University named after N.I. Lobachevsky (603022, Nizhny Novgorod, Gagarin Ave., 23; e-mail: irinafilipova@yandex.ru).

Recommended citation

Begishev I.R., *Filipova I.A.* Protection of employees' personal data in the context of the spread of algorithmic management based on court practice. Kazan University Law Review. 2025; 4 (10): 190–212. DOI: 10.30729/2541-8823-2025-10-4-190-212.

CONFERENCE REVIEWS

Zilya Miftakhutdinova

5th year, specialist's degree of the Kazan Federal University

OUTCOMES OF THE 10TH INTERNATIONAL SCIENTIFIC AND PRACTICAL CONVENTION OF STUDENTS AND POSTGRADUATES "VECTOR OF LAW: GLOBAL CHALLENGES AND THE NATIONAL CODE"

DOI: 10.30729/2541-8823-2025-10-4-213-215

Abstract. *The article is devoted to the outcomes of the 10th International Scientific and Practical Convention of Students and Postgraduates "Vector of Law: Global Challenges and the National Code", held on November 28–29 at Kazan (Volga Region) Federal University. The key events, award ceremonies, opening and closing sessions are described in detail. The article analyzes the geography of the convention and the organizational process itself. The geographical representation of the participants is reviewed — it included more than 250 students from 20 leading law universities of Russia and neighboring countries. Special attention is given to the discussion of major issues in contemporary jurisprudence, the search for innovative approaches, and the development of proposals for transforming modern law. The significance of the convention as a platform that unites young scholars and experienced researchers is emphasized, providing a productive space for the exchange of knowledge and best practices in organizing similar events.*

Keywords: *global challenges, national code, students, platform, lawyers, law, professional skills, experience*

On November 28–29, the 10th International Scientific and Practical Convention of Students and Postgraduates "Vector of Law: Global Challenges and the National Code" took place within the walls of Kazan (Volga Region) Federal University. The event became a platform for the active exchange of knowledge and professional skills among students and postgraduates of law faculties from leading universities of Russia and neighboring countries.

The main goal of the convention was to create a discussion field around the main trends in the evolution of legal norms and principles under modern global challenges. The emphasis was placed on the development of national legal standards reflecting the specificity of the Russian state and the current realities of the international legal order.

The work of the Convention was organized into 14 thematic sections where students presented their research papers aimed at identifying promising directions for the reform of legislation and improving the efficiency of the justice system. Among the key elements of the event, particular attention was drawn to the tradition of holding the All-Russian Model Judicial Process — "All-Russian Moot Court", which allowed future lawyers to experience the atmosphere of real court proceedings. Such a format helps students develop practical problem-solving skills and strengthens public confidence in the institutions of justice.

More than 250 students and postgraduates from twenty leading Russian universities participated in the International Convention, representing Moscow, Saint Petersburg, Yekaterinburg, Perm, Kaliningrad, Saratov, Samara, and many other cities. In addition to Russian delegates, teams from China, Kazakhstan, and Azerbaijan also attended the event. The representation of regional characteristics made it possible to form a comprehensive picture of the state of legal education and professional training of law students in Russia.

The first day began with the official opening ceremony. In the afternoon, an open lecture was held by Candidate of Legal Sciences and Head of the Foundation for the Development of the Legacy of Professor Mikhail Treushnikov — Leonid Afanasyev. The lecture was dedicated to the heritage of the distinguished scholar and Professor Mikhail Treushnikov and his contribution to Russian legal thought. The day continued with engaging workshops delivered by renowned experts in the field. Such sessions contribute to a deeper understanding among students of legal mechanisms and the latest methods of studying normative legal acts.

The second day launched the active work of the sections, where participants could present their research papers and discuss the most pressing issues of modern law. In the afternoon, the results of the student research competitions were summed up, and the best researchers of the convention were awarded.

This year, the International Scientific and Practical Convention of Students and Postgraduates "Vector of Law: Global Challenges and the National Code" was held for the tenth time. At the official opening, which took place at the Faculty of Law of Kazan (Volga Region) Federal University, the participants and guests were welcomed by First Vice-Rector — Vice-Rector for Research Dmitry Tayursky, Dean of the Faculty of Law Lilia Bakulina, and other honored guests. They expressed confidence that the 10th Convention would become a bright and memorable event in the lives of all participants and make a significant contribution to the development of legal education in Russia. The award ceremony and official closing were held on the second day of the event.

The title partner of the event was Gorodets Publishing House — one of the leading publishing companies in Russia. The general partner was the Yalilov & Partners Law Firm, with additional support from the Institute for Legal Literacy (ANO). The informational partners of the convention included the International Association of Lawyers and Consultants, Pravo.ru, and the academic journal Herald of Civil Procedure.

The organization of the 10th International Scientific and Practical Convention of Students and Postgraduates “Vector of Law: Global Challenges and the National Code” demonstrated a high level of youth engagement with legal science and practice. The event reaffirmed its effectiveness as a tool for updating the methodology of legal education and emphasized the importance of regular exchange of ideas and experiences within the professional legal community.

Information about the author

Zilya Miftakhutdinova — 5th year, specialist’s degree of the Kazan Federal University (e-mail zilyakkamilevna2004@gmail.com).

Recommended citation

Miftakhutdinova Z. K. Outcomes of the 10th International Scientific and Practical Convention of Students and Postgraduates “Vector of Law: Global Challenges and the National Code”. Kazan University Law Review. 2025; 4 (10): 213–215. DOI: 10.30729/2541-8823-2025-10-4-213-215.

The inaugural issue of the journal was launched by the Law Faculty of Kazan Federal University in December 2016. ISSN number: 2541-8823.

The journal is printed in English and comes out in four issues per year.

The journal has an International Editorial Council and a Russian Editorial Board. All articles are reviewed by a professional copyeditor whose native language is English.

Requirements for submissions:

- The journal accepts articles on fundamental issues of law not previously published elsewhere. The content of articles should reflect the author's original academic approach and developed doctrine of jurisprudence.
- Articles must be submitted in the English language only.
- Recommended number of words/pages: the journal uses the character count method. The total length of the article (including the title, abstract, keywords, introduction, text, conclusions, acknowledgements, literature) is from 15,000–100,000 characters with spaces (9–20 pages).
- Articles must include an abstract with 150–250 words and a list of at least five Keywords.
- The section "Information about the author" must appear at the end of the article: it should contain the surname and name of the author, title of the author, place of work (or study), postal address, telephone number and e-mail address.
- For postgraduate students: please attach (as an image file) a review on the article written by a certified supervisor.
- Deadlines for submission of articles:

  Issue No. 1 – January 15 (launch of printed issue is March);
  Issue No. 2 – April 15 (launch of printed issue is June);
  Issue No. 3 – June 15 (launch of printed issue is September);
  Issue No. 4 – October 15 (launch of printed issue is December).
- Citation format: footnotes should conform to the 20th edition of The Bluebook: A Uniform System of Citation.

The journal staff may be contacted via e-mail at: kulr.journal@gmail.com.

To find more information about the journal:

Kazan
Federal
University

FACULTY
of Law

Faculty of Law welcomes everyone applying for master's degree!

MASTER'S PROGRAMS 2025–2026

- Anti-corruption studies
- European and international business law (in English)
- International human rights law
- Legal analytics
- Legal support of business
- Preliminary investigation and criminal justice
- Litigator in civil, arbitration and administrative proceedings
- Private and business law
- Legal protection of the rights of citizens in criminal proceedings
- Lawyer in governmental authority
- Lawyer in digital economy

Kazan University Law Review 2025–2026

Dear colleagues,

On behalf of the editorial board of the international scientific journal Law Review, we cordially congratulate you on the New Year!

The year ending has become another bright page in our fruitful cooperation.

We are sincerely glad that for so long we have been united by professional trust, scientific interest and a common commitment to the development of the scientific community. Thanks to your participation, high standards of academic work and constant support, our journal continues to strengthen its position in the international academic community.

We deeply appreciate every contribution — publications, peer reviews, joint projects, and expert opinions — that helps us collectively advance science, expand the horizons of legal research, and create a platform for dialogue between scientists from around the world.

May the 2026 year bring you new ideas, inspiration, scientific achievements and professional success. We hope to further strengthen our cooperation, launch new joint initiatives and maintain the friendly and at the same time professional ties that are so important to all of us.

We wish you well-being, good health, harmony and success in all your endeavors. May the New Year be full of joyful events, opening up new perspectives and opportunities for you.

Sincerely,
Editorial Board of the Kazan University Law Review

P.S. We attach a calendar for 2026 with scientists from the modern Kazan Law School — a sign of our appreciation and a source of inspiration for the year ahead.

CALENDAR 2026

Kazan University

LAW REVIEW

e-mail: kulr.journal @gmail.com

02.01.
Малый Александр Федорович
д-р юрид. наук, проф.
Maly Alexander Fedorovich
Advanced Doctor in Law, Prof.

05.01.
Гатауллин Анас Газизович
д-р юрид. наук, проф.
Gataullin Anas Gazizovich
Advanced Doctor in Law, Prof.

27.01.
Давлетгильдеев Рустем Шамилевич
д-р юрид. наук, проф.,
зав. каф. теории и истории
государства и права
Davletgildeev Rustem Shamilevich
Advanced Doctor in Law, Prof.,
Head of the Dept. of Theory and
History of State and Law

29.01.
Бакулина Лилия Талгатовна
д-р юрид. наук, проф.,
декан Юридическогофакультета
Bakulina Liliya Talgatovna
Advanced Doctor in Law, Prof.,
Dean of the Faculty of Law

31.01.
Сафин Завдат Файзрахманович
д-р юрид. наук, проф., зав. каф.
экологического, трудового права
и гражданского процесса
Safin Zavdat Fayzrakhmanovich
Advanced Doctor in Law, Prof.,
Head of the Dept. of
Environmental and Labor Law
and Civil Procedure

JANUARY

SUN	MON	TUE	WED	THU	FRI	SAT
28	29	30	31	1	[✓ 2]	3
4	[✓ 5]	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	[✓ 27]	28	[✓ 29]	30	[✓ 31]
1	2	3	4	5	6	7

Kazan University
LAW REVIEW

10.02.
Железнов Борис Леонидович
д-р юрид. наук, проф.,
академик Российской Академии Наук
Zheleznov Boris Leonidovich
Advanced Doctor in Law, Prof.,
Academician of the Russian Academy
of Sciences

11.02.
Сафин Ленар Ринатович
канд. юрид. наук, доц., ректор КФУ
Safin Lenar Rinatovich
PhD in Law, Assoc. Prof., Head of KFU

14.02.
Тарханов Ильдар Абдулхакович
д-р юрид. наук, проф.,
научный руководитель
юрид. факультета
Tarkhanov Ildar Abdulkhakovich
Advanced Doctor in Law, Prof.,
Academic Supervisor of
the Faculty of Law

15.02.
Валеев Дамир Хамитович
д-р юрид. наук, проф., главный редактор
журнала Kazan University Law Review
Valeev Damir Khamitovich
Advanced Doctor in Law, Prof.,
Editor-in-Chief of the Kazan University
Law Review

FEBRUARY

SUN	MON	TUE	WED	THU	FRI	SAT
1	2	3	4	5	6	7
8	9	[✓ 10]	[✓ 11]	12	13	[✓ 14]
[✓ 15]	16	17	18	19	20	21
22	23	24	25	26	27	28
1	2	3	4	5	6	7
8	9	10	11	12	13	14

Kazan University
LAW REVIEW

13.03.
Лунева Елена Викторовна
д-р юрид. наук, проф.
Luneva Elena Viktorovna
Advanced Doctor in Law, Prof.

14.03.
Нуриев Анас Гаптрауфович
д-р юрид. наук, доц.
Nuriyev Anas Gaptraufovich
Advanced Doctor in Law, Assoc. Prof.

MARCH

SUN	MON	TUE	WED	THU	FRI	SAT
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	**16**	17	18	19	**20**	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Kazan University
LAW REVIEW

12.04.

Муратова Надежда Георгиевна

д-р юрид. наук, проф.

Muratova Nadezhda Georgievna

Advanced Doctor in Law, Prof.

27.04.

Валиев Рафаиль Газизуллович

д-р юрид. наук, проф.

Valiev Rafail Gazizullovich

Advanced Doctor in Law, Prof.

APRIL

SUN	MON	TUE	WED	THU	FRI	SAT
29	30	31	1	2	3	4
5	6	7	8	9	10	11
[✓ 12]	13	14	15	16	17	18
19	20	21	22	23	24	25
26	[✓ 27]	28	29	30	1	2
3	4	5	6	7	8	9

Kazan University
LAW REVIEW

01.05.
Михайлов Андрей Валерьевич
д-р юрид. наук, доц.,
зав. каф. предпринимательского и энергетического права
Mikhaylov Andrey Valeryevich
Advanced Doctor in Law, Assoc. Prof.,
Head of the Dept. of Business and Energy Law

04.05.
Ситдикова Роза Иосифовна
д-р юрид. наук, проф.
Sitdikova Roza Iosifovna
Advanced Doctor in Law, Prof.

12.05.
Тюрина Наталия Евгеньевна
д-р юрид. наук, проф.
Tyurina Natalia Evgenievna
Advanced Doctor in Law, Prof.

20.05.
Клюкова Марина Евгеньевна
канд. юрид. наук, доц., зав. каф. уголовного процесса и криминалистики
Klyukova Marina Evgenievna
PhD in Law, Assoc. Prof.,
Head of the Dept. of Criminal Procedure and Forensics

MAY

SUN	MON	TUE	WED	THU	FRI	SAT
26	27	28	29	30	[✓ 1]	2
3	[✓ 4]	5	6	7	8	9
10	11	[✓ 12]	13	14	15	16
17	18	19	[✓ 20]	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

Kazan University
LAW REVIEW

19.06.
Степаненко Равия Фаритовна
д-р юрид. наук, проф.
Stepanenko Raviya Faritovna
Advanced Doctor in Law, Prof.

29.06.
Салиева Роза Наильевна
д-р юрид. наук, проф.
Saliyeva Roza Nailevna
Advanced Doctor in Law, Prof.

JUNE

SUN	MON	TUE	WED	THU	FRI	SAT
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	[✓ 19]	20
21	22	23	24	25	26	27
28	[✓ 29]	30	1	2	3	4
5	6	7	8	9	10	11

Kazan University
LAW REVIEW

13.07.
Курдюков Геннадий Иринархович
д-р юрид. наук, проф.
Kurdyukov Gennady Irinarkhovich
Advanced Doctor in Law, Prof.

15.07.
Талан Мария Вячеславовна
д-р юрид. наук, проф.
Talan Maria Vyacheslavovna
Advanced Doctor in Law, Prof.

20.07.
Загидуллин Марат Рашитович
д-р юрид. наук, проф.
Zagidullin Marat Rashitovich
Advanced Doctor in Law, Prof.

23.07.
Султанов Евгений Батырович
канд. юрид. наук, доц., зав. каф.
конституционного и
административного права
Sultanov Evgeny Batyrovich
PhD in Law, Assoc. Prof.,
Head of the Dept. of
Constitutional and Administrative Law

29.07.
Абдуллин Адель Ильсиярович
д-р юрид. наук, проф.,
зав. каф. международного права
Abdullin Adel Ilsiyarovich
Advanced Doctor in Law, Prof.,
Head of the Dept. of International Law

JULY

SUN	MON	TUE	WED	THU	FRI	SAT
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	[✓ 13]	14	[✓ 15]	16	17	18
19	[✓ 20]	21	22	[✓ 23]	24	25
26	27	28	[✓ 29]	30	31	1
2	3	4	5	6	7	8

Kazan University
LAW REVIEW

02.08.
Курманов Мидхат Мазгутович
д-р юрид. наук, проф.
Kurmanov Midkhat Mazgutovich
Advanced Doctor in Law, Prof.

12.08.
Мишин Андрей Викторович
д-р юрид. наук, проф.
Mishin Andrey Viktorovich
Advanced Doctor in Law, Prof.

17.08.
Кешнер Мария Валерьевна
д-р юрид. наук, проф.
Keshner Maria Valeryevna
Advanced Doctor in Law, Prof.

19.08.
Валеев Револь Миргалимович
проф.-консультант
Valeev Revol Mirgalimovich
Consulting Prof.

29.08.
Голубев Станислав Игоревич
д-р юрид. наук, проф.
Golubev Stanislav Igorevich
Advanced Doctor in Law, Prof.

AUGUST

SUN	MON	TUE	WED	THU	FRI	SAT
26	27	28	29	30	31	1
[✓ 2]	3	4	5	6	7	8
9	10	11	[✓ 12]	13	14	15
16	[✓ 17]	18	[✓ 19]	20	21	22
23	24	25	26	27	28	[✓ 29]
30	31	1	2	3	4	5

Kazan University
LAW REVIEW

27.09.

Хусаинов Зуфар Фаатович

д-р юрид. наук, проф.

Khusainov Zufar Faatovich

Advanced Doctor in Law, Prof.

SEPTEMBER

SUN	MON	TUE	WED	THU	FRI	SAT
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

Kazan University
LAW REVIEW

13.10.
Погодин Александр Витальевич
д-р юрид. наук, проф.
Pogodin Alexander Vitalevich
Advanced Doctor in Law, Prof.

14.10.
Антонов Игорь Олегович
д-р юрид. наук, доц.
Antonov Igor Olegovich
Advanced Doctor in Law,
Assoc. Prof.

16.10.
Епихин Александр Юрьевич
д-р юрид. наук, проф.
Epikhin Alexander Yuryevich
Advanced Doctor in Law, Prof.

27.10.
Арсланов Камиль Маратович
д-р юрид. наук, проф., зав.
каф. гражданского права
Arslanov Kamil Maratovich
Advanced Doctor in Law, Prof.,
Head of the Dept. of Civil Law

OCTOBER

SUN	MON	TUE	WED	THU	FRI	SAT
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	[✓ 13]	[✓ 14]	15	[✓ 16]	17
18	19	20	21	22	23	24
25	26	[✓ 27]	28	29	30	31
1	2	3	4	5	6	7

Kazan University
LAW REVIEW

01.11.
Сундуров Федор Романович
д-р юрид. наук, проф.
Sundurov Fyodor Romanovich
Advanced Doctor in Law, Prof.

09.11.
Ибрагимова Елена Михайловна
д-р пед. наук, проф., зав. каф.
теории и методики обучения праву
Ibragimova Elena Mikhailovna
Advanced Doctor in Pedagogical
Sciences, Prof., Head of the Dept. of
Theory and Methods of Teaching Law

16.11.
Челышев Михаил Юрьевич
д-р юрид. наук, проф.
Chelyshev Mikhail Yuryevich
Advanced Doctor in Law, Prof.

24.11.
Нигматуллина Эльмира Фаатовна
д-р юрид. наук, проф.
Nigmatullina Elmira Faatovna
Advanced Doctor in Law, Prof.

NOVEMBER

SUN	MON	TUE	WED	THU	FRI	SAT
[✓ 1]	2	3	4	5	6	7
8	[✓ 9]	10	11	12	13	14
15	[✓ 16]	17	18	19	20	21
22	23	[✓ 24]	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Kazan University
LAW REVIEW

04.12.
Шайхутдинова Гульнара Раифовна
д-р юрид. наук, проф.
Shaikhutdinova Gulnara Raifovna
Advanced Doctor in Law, Prof.

06.12.
Васькевич Владимир Петрович
д-р юрид. наук, проф.
Vaskkevich Vladimir Petrovich
Advanced Doctor in Law, Prof.

25.12.
Хабибуллина Гульнара Рушановна
д-р юрид. наук, проф.
Khabibullina Gulnara Rushanovna
Advanced Doctor in Law, Prof.

DECEMBER

SUN	MON	TUE	WED	THU	FRI	SAT
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

Kazan University
LAW REVIEW

KAZAN UNIVERSITY LAW REVIEW
Volume 10, Autumn 2025, Number 4

Release date 23.12.2025
Form. 70x100 1/16. Volume 5,5 printed sheets
Circulation 100

Published by LLC “Prospekt”,
Russia, Moscow, Borovaya st., 7, building 4

ООО «Проспект»,
Россия, г. Москва, ул. Боровая, д. 7, стр. 4

Свободная цена