Public Law Challenges in Protecting Human Digital Rights in the Age of Artificial Intelligence

1. Mahdi Rajaei : Assistant Professor, Department of Public Law, Faculty of Law, University of Qom, Qom, Iran
2. Ali Amiri *: Master's Student, Department of Public Law, Faculty of Law, University of Qom, Qom, Iran

*Correspondence: a.amiri@stu.qom.ac.ir

Abstract

The increasing use of artificial intelligence and its application in various fields have created both opportunities and challenges, which also exist in the application of artificial intelligence in public law contexts. The sum of these opportunities and challenges can be studied as digital human rights in the field of public law. In a way, these rights define the operational framework of artificial intelligence in this field. In this regard, the opportunities created by artificial intelligence should first be examined as part of human digital rights. Then, the challenges arising from artificial intelligence should be analyzed and identified as among the negative rights against which humanity must be protected. In this regard, challenges such as algorithmic transparency, accountability, privacy, and jurisdiction issues are raised, and the need to strike a balance between this new tool and security and privacy is emphasized. This research aims to explore the concept of human digital rights in the context of artificial intelligence in public law and to examine how they can be effectively protected. In order to answer this question, this article, relying on a descriptive analytical method, first provides recommendations for policymakers, experts, and researchers, and tries to overcome the challenges in this field, including cybersecurity, privacy, and decision-making, which are considered among the most challenging concepts in public law, by proposing macro-policies. Therefore, by developing up-to-date laws and regulations that align with digital advances, we can reap the benefits of artificial intelligence in enhancing public rights.

Keywords: Public Law, Artificial Intelligence, Digital Human Rights, Cyber, Data Protection, Administrative Transparency.

Received: 08 May 2025
Revised: 17 July 2025
Accepted: 25 July 2025
Published: 01 August 2025

Citation: Rajaei, M., & Amiri, A. (2025). Public Law Challenges in Protecting Human Digital Rights in the Age of Artificial Intelligence. *Legal Studies in Digital Age,* 4(3), 1-7.

1. Introduction

Today, the use of modern digital technologies has created one of the requirements for transformation in modern society and governments. The digital revolution, as a factor of dynamic development, has led to the creation of a digital economy, the development of the foundations of digital law, and a new configuration of social relations based on the use of the Internet, social networks, and other information and communication technologies. Modern digital technologies are shaping a new way of production in which humans do not participate directly, and cyberspace itself makes decisions and presents them to its users. This creates the prerequisites for the transition from this period to a new form of social interaction, in which the new law plays an important role in regulating emerging relationships (Hyliaka, 2021). Digital transformation has a direct impact on the implementation of fundamental human rights. It helps the emergence of new human and civil rights as a participant in the global information and digital space, which can create a set of human rights in the digital arena (Shaelou & Razmetaeva, 2023). The results of digitalization necessitate an understanding and the formulation of appropriate legal mechanisms to regulate, implement, and protect existing and emerging human rights, promoting sustainable socio-economic development and ensuring the implementation of fundamental and civil human rights and freedoms (Ahmad et al., 2025; Rajaei & Amiri, 2025). In the current digital age, public law, which governs and regulates the relationship between the government and its citizens, has undergone significant changes. In this way, with the emergence of new digital technologies, the traditional definition of public rights changes. Therefore, privacy, cybersecurity, and artificial intelligence should be compatible with public rights (Bakiner, 2023). This approach presents numerous challenges that must be addressed or corrected. With the emergence and rapid development of new technologies, privacy threats are also increasing at a rapid pace. The right to privacy is one of the fundamental rights stipulated in human rights documents. With the increasing digitalization of modern life, privacy protection has become more challenging, and in many cases, new examples have emerged or existing ones have evolved to violate it, often allowing governmental and non-governmental organizations to interfere with citizens' privacy. Even those laws that regulate the possibility of such interference and determine cases for granting permission to the relevant authorities are not keeping pace with the rapid development of technology. The protection methods provided by the current law do not meet the requirements of the modern world, and there is a need to review the mechanisms of legal regulation and professional legal awareness in general (Klitou, 2014; Nyst & Falchetta, 2017). On the other hand, in the rapidly evolving digital landscape, the field of cyber law has emerged as an important and interesting legal field. With increasing dependence on technology, challenges and legal implications related to cybersecurity, data privacy, intellectual property rights, and online sovereignty also increase (Aleksandrovich, 2023). The potential of artificial intelligence to make fundamental changes in behavior, daily routines, and improve efficiency in various fields is obvious. However, AI systems typically require significant data collection and analysis, which raises issues regarding the protection of individuals' privacy, a fundamental and relevant element of human rights (Ahmad et al., 2025). Therefore, based on the stated information, a set of legal rules and principles governing the relations between the government, public institutions, and citizens in the digital space constitutes a new definition of public law (Rostovska et al., 2024). Based on what has been stated, the challenges of public law in the digital age can be examined in three areas: (1) privacy and data protection, (2) cybersecurity, and (3) the use of artificial intelligence in sovereign decision-making. Therefore, the following examines each of these areas and presents the challenges, opportunities, and appropriate solutions for each. In this regard, the upcoming research aims to examine the existing challenges and new opportunities in the digital age for enhancing the improvement and efficiency of public law, and to develop solutions to address these challenges, thereby improving the status of digital human rights in the field of public law.

2. Challenges facing public law in protecting human digital rights

As stated, the development of the digital space and the addition of artificial intelligence to human possibilities, in addition to the privileges it creates for humans, will dramatically change their relationships with citizens and sovereignty, which requires a reexamination of the components of human rights in emerging areas. In this regard, it is necessary first to identify these challenges.

2.1. Privacy and data protection

Self-learning mechanisms drive artificial intelligence technology. These self-learning mechanisms can adapt their programmed algorithms in response to the input data. The important point is that although algorithms may be transparent to their designers, after the system has gone through hundreds, thousands, or even millions of recursive self-programming patterns, even the system programmers no longer know which types of data were processed in what way, which inferences were drawn from which data correlations, and how specific data were weighted (Poscher, 2021). This is why artificial intelligence, due to its lack of transparency, poses problems for the traditional understanding and treatment of the right to data protection. These issues are reflected in the transparency requirements of the General Data Protection Regulation, which is primarily based on the traditional concept of the fundamental right to data protection (Rajaei & Amiri, 2024).

On the other hand, the decisions made by artificial intelligence cannot be evaluated due to the lack of transparency in the decision-making process. It is unclear what presuppositions led to this decision. Therefore, it is not possible to examine those presuppositions to be sure of the decision made. Therefore, it can be said that the most significant challenge for public law in protecting human digital rights in the age of artificial intelligence is the concerns arising from personal security issues, invasion of privacy, and the risk of sensitive data misuse. Intelligent surveillance, including facial recognition systems, online surveillance, and data tracking, can enhance public safety, but it also poses significant privacy challenges. While the protection of this right should be considered a fundamental right, individuals should not be subjected to such surveillance. Therefore, the challenge raised should be carefully assessed. In terms of privacy protection, a balance must be reached between the duality of protecting public security and paying attention to privacy that ensures both. Additionally, one of the other prominent challenges that can arise from the distortion of privacy is the erosion of public trust in sovereignty. Because people react negatively to constant monitoring and the distortion of their privacy, they lose their trust in the sovereignty.

Table 1. Studies on Privacy and Data Protection in the Age of Artificial Intelligence

Reference	Study Objective	Challenges	Solutions	Results
(Solove, 2025)	Creating a fundamental understanding of the intersection between AI and privacy	There is a lack of privacy legislation that addresses AI privacy issues	Conceptualization and codification of law	Misguided approaches to privacy law and other uncorrected flaws are particularly ill-suited for AI
(Renuka et al., 2025)	Review of data privacy in the digital age	Legal and ethical challenges arising from technological advances and data-driven processes	The impact of legal frameworks with a focus on GDPR and similar regulations	The importance of strong legal frameworks and ethical guidelines to protect data privacy while promoting responsible data management practices
(Yanamala & Suryadevara, 2023)	The intersection of artificial intelligence and data protection with a focus on regulatory frameworks, ethical considerations, and technological innovations	Ethical implications of decision-making based on artificial intelligence and emerging technologies such as federated learning and differential privacy	The dynamic interplay between regulatory frameworks, technological innovations, and ethical imperatives in navigating data protection challenges in artificial intelligence-based ecosystems	Combining empirical evidence and theoretical insights helps advance knowledge and inform evidence-based policy-making in promoting a safe, fair, and ethical digital future

To promote and maintain the security of privacy and data, and to ensure the security of citizens' information, encryption and electronic authentication can be considered suitable solutions. Additionally, digital identity management systems are used to prevent fraud and misuse of individual information. In this regard, governments also must clearly state how data is collected and used. The government should establish strict laws to protect data. To prevent any misuse of data, a governing body should be created to oversee the performance of security organizations. Access to individuals' data can be limited using encryption.

2.2. Cybersecurity

The concept of cybersecurity in the context of public law refers to the set of measures, policies, and mechanisms that governments adopt to protect critical information infrastructure, maintain data confidentiality and integrity, and safeguard citizens' digital freedoms. Since the government is primarily responsible for ensuring public order, security, and rights, its role in securing cyberspace and confronting cyber threats is particularly prominent. From the perspective of public law, cybersecurity is not just a technical issue, but also has important political, social, economic, and human rights dimensions. Any governmental intervention in this area must be accompanied by adherence to democratic principles, transparency, accountability, and proportionality, as security measures, in the absence of legal oversight, may become a tool to suppress digital freedoms and violate the fundamental rights of citizens. Therefore, in the public law approach, cybersecurity is understood in the balance between the power of sovereignty to ensure national security and protect the legitimate rights and freedoms of cyberspace users. This balance requires the establishment of laws that are intelligent, transparent, flexible, and consistent with international human rights standards. Establishing and strengthening cybersecurity is a crucial necessity in public law. Considering the increase in cyberattacks on government critical infrastructure, the challenges raised must be analyzed, as national security is of great importance in public law (Aleksandrovich, 2023).

Table 2. Studies on Cybersecurity in the Age of Artificial Intelligence

Reference	Study Objective	Challenges	Solutions	Results
(Ashraf & Mustafa, 2025)	The intersection of artificial intelligence and cyber law	Legal and regulatory challenges such as algorithmic transparency, accountability, privacy, and jurisdictional issues	Applications of artificial intelligence in cybersecurity, such as threat detection, automated incident response	The need to balance cybersecurity and privacy
(Ghosh et al., 2025)	Investigating cyberbullying in the digital age	Anonymity and ease of access, harassment, disclosure of personal information, and dissemination of misinformation	Comprehensive intervention strategies, awareness programs, and digital literacy initiatives to protect users	Preventing severe emotional and psychological harm
(Imam & Naz, 2024)	Cyberbullying in the digital age	Anonymity and ease of access, harassment, disclosure of personal information, and dissemination of misinformation	Technological solutions, such as AI-based detection and public awareness campaigns, along with parental involvement	Comprehensive legal, educational, and technological strategies to protect victims and ensure cyberbullies are held accountable
(Aleksandrovich, 2023)	Examining the legal and regulatory aspects of cyber law in the digital age	Challenges and issues related to privacy and data security, and existing legal frameworks to address cyber law issues	Critical analysis, practical and legal consequences of cyber law, and policy considerations	The importance of strong cyber law regulations to ensure a safe and trustworthy digital environment

Given that the use of digital technologies, if used correctly, can create major changes in administrative transparency; however, it requires human resource training, accurate planning, and ensuring cybersecurity. Therefore, one should not rely completely on artificial intelligence in public law, and human judgments and flexibility in the legal system should be prioritized. Based on what has been stated, it can be said that cybersecurity, as one of the areas of security, is considered a government responsibility. Therefore, it can be considered one of the areas of digital human rights. The nature of this right can be considered a negative right. As stated, this right is a subset of the field of security, which is considered one of the first-generation rights and a negative right. This means that the government is responsible for ensuring these rights, not creating obstacles for people to use this area. Based on this opinion, the government, by not interfering in this area, provides citizens with the opportunity to benefit from it. As part of the cybersecurity area, restrictive measures and government interference are involved. The absence of these acts provides some degree of security. However, part of the area of cybersecurity refers to the cybersecurity of the community. On the one hand, attacks by foreign enemies can disrupt this space and exploit personal and private information, causing harm to individuals and the overall cyber social space. In this area, of course, since one of the areas related to social security is compromised, the sovereignty is obliged to protect the country's cybersecurity. Therefore, cybersecurity can be examined from two aspects. The first is the part related to the cybersecurity of citizens against the sovereignty, where the field of public law regulates these relations and determines the relationship between the sovereignty and the people in this area. However, the other area of cybersecurity has a supranational aspect, which is raised in the context of national security. This responsibility falls to the government, and the government's authority in this regard has a positive aspect, meaning that the government must defend national cybersecurity against these threats.

2.3. Artificial Intelligence in Decision Making

Another area that needs to be considered regarding digital human rights is the use of this space, and especially the artificial intelligence platform, in administrative and judicial decision-making, as the use of artificial intelligence can lead to violations of citizens' rights. Among the challenges raised is the lack of transparency of artificial intelligence algorithms and the impossibility of protesting artificial intelligence decisions, which should be addressed in public law (Mohebbi & Amiri, 2025). Also, decision-making with artificial intelligence gives the impression that there is no fair access. On the other hand, the digitalization of public services can increase the efficiency and transparency of the government. Additionally, the use of artificial intelligence can help prevent administrative corruption in decision-making (Cetina Presuel & Martinez Sierra, 2024; Zuwanda et al., 2024). In legal oversight, AI can help with decision-making by quickly analyzing laws.

However, in some cases, the use of AI can lead to a decrease in public trust and a violation of citizen rights. Artificial intelligence can play a significant role in enhancing administrative transparency, providing high efficiency, quick responses, and increasing public participation. Additionally, with free access to citizens' information and data from artificial intelligence, they can see the outcome of the decision. Another advantage of artificial intelligence is its ability to reduce administrative corruption. It also shows transparency in all decision-making. Accountability, improvement, and acceleration of the response and decision-making process are among the strengths of artificial intelligence in public law. Also, all citizens can report their complaints and administrative violations online and have AI provide conclusions in the shortest possible time. Artificial intelligence can also identify and correct inefficiencies in human decision-making. Another important challenge is the lack of fair access to artificial intelligence for all citizens across different regions in the administrative decision-making process. Additionally, gaining public trust in this type of decision is another challenge.

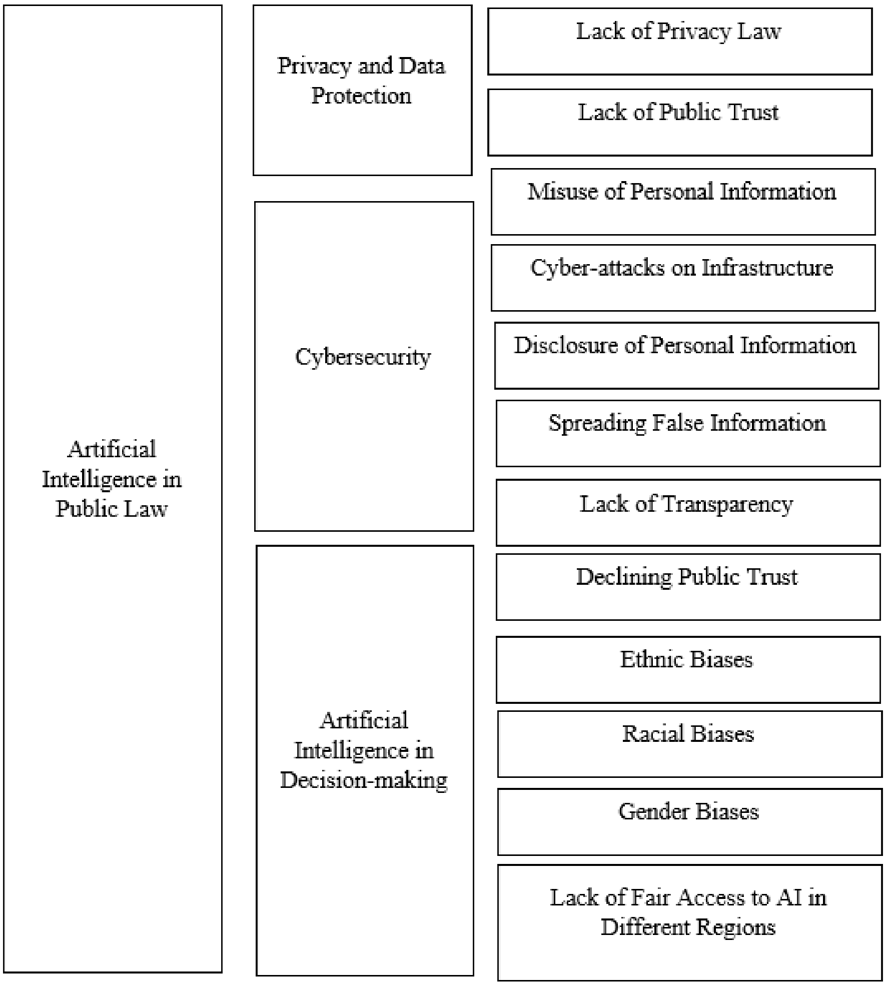
Artificial Intelligence in Public Law
Privacy and Data Protection
Cybersecurity
Artificial Intelligence in Decision-making
Lack of Privacy Law
Lack of Public Trust
Misuse of Personal Information
Cyber-attacks on Infrastructure
Disclosure of Personal Information
Spreading False Information
Lack of Transparency
Declining Public Trust
Ethnic Biases
Racial Biases
Gender Biases
Lack of Fair Access to AI in Different Regions

Figure 1. Public law challenges in protecting human digital rights in the age of artificial intelligence.

3. Ethical considerations

In the current digital age, adhering to ethical considerations when using artificial intelligence is of great importance. Although the field of ethics differs from the field of law, due to the intertwining and close relationship between these two fields, it can serve as a foundation for the application of artificial intelligence. The use of the artificial intelligence platform requires more than anything else the creation of a social movement and cultural development in this regard, and this cannot be achieved only through the legislative system, because this requires a series of self-controls and internal controls, which is achieved by paying attention to the field of ethics. It is the field of social ethics that can shape this culture in society, and the way artificial intelligence is used and how it is perceived in society becomes a part of that culture. Ethics can play an irreplaceable and important role in the field of creating culture, a process that leads to gaining the public trust of the people.

The debate over the fairness of AI decisions in public law and the issue of injustice in AI decision-making are other aspects in which the role of ethics can be observed. In many cases, legal action cannot achieve fairness and justice in all instances. However, ethics can achieve this important goal through the self-control it fosters in the individual. In other words, when the law cannot fully play a role in establishing justice and fairness, an individual's internal control, based on ethics and moral requirements, can achieve this. Given that artificial intelligence makes decisions based on the information provided, possible errors caused by biases and discrimination in the data it receives from human resources must be examined. This factor can also be considered as one of the platforms for the intervention of ethics in the use of artificial intelligence.

These damages and challenges can only be realized through the observance of ethical issues and internal controls. Racial, ethnic, and gender biases can also be addressed with the help of ethical controls and guarantees of ethical implementation. In the area of privacy and respect for it, ethics and adherence to its norms are among the most important means of controlling this area and preventing unnecessary intrusion, working alongside legal mechanisms to ensure protection.

4. Conclusion

Cybersecurity, privacy, and decision-making by artificial intelligence are among the most challenging concepts considered in public law, particularly in ensuring digital human rights. These challenges can help realize the maximum digital human rights by strengthening public rights through the development of new laws and regulations in response to digital developments. The challenges of public law in protecting human digital rights in the age of artificial intelligence can be addressed with intelligent solutions that lead to improved efficiency of the public law system, through increased public trust, transparency in accountability, equality, justice, privacy protection, increased national security, and benefiting from ethical controls and the use of ethical enforcement guarantees. Appropriate solutions for securing human digital rights can be promoted through these means.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Ahmad, N., Ali, A. W., & bin Yussof, M. H. B. (2025). The Challenges of Human Rights in the Era of Artificial Intelligence. *Uum Journal of Legal Studies*, *16*(1), 150-169. https://doi.org/10.32890/uumjls2025.16.1.9

Aleksandrovich, L. A. (2023). Cyber Law: Addressing Legal Challenges in the Digital Age. *Uzbek Journal of Law and Digital Policy*, *1*(3), 12. https://doi.org/10.59022/ujldp.92

Ashraf, Z. A., & Mustafa, N. (2025). AI and Cyber Laws. In *Intersection of Human Rights and AI in Healthcare*. IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7051-3.ch015

Bakiner, O. (2023). The promises and challenges of addressing artificial intelligence with human rights. *Big Data & Society*, *10*(2), 20539517231205476. https://doi.org/10.1177/20539517231205476

Cetina Presuel, R., & Martinez Sierra, J. M. (2024). The adoption of artificial intelligence in bureaucratic decision-making: A Weberian perspective. *Digital Government: Research and Practice*, *5*(1), 1-20. https://doi.org/10.1145/3609861

Ghosh, R., Malhotra, M., & Kumar, N. (2025). Cyber Bullying in the Digital Age: Challenges, Impact, and Strategies for Prevention. In *Combating Cyberbullying With Generative AI* (pp. 151-180). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0543-1.ch006

Hyliaka, S. (2021). Human rights in the digital age: Challenges, threats and prospects. *Науковий юридичний журнал*, *28*(1), 16. https://doi.org/10.37635/jnalsu.28(1).2021.15-23

Imam, S. K., & Naz, T. (2024). Cyberbullying: Legal Challenges and Societal Impacts in the Digital Age. *Pakistan Social Sciences Review*, *8*(4), 392-407. https://doi.org/10.35484/pssr.2024(8-IV)31

Klitou, D. (2014). Privacy-invading technologies and privacy by design. In *Information Technology and Law Series* (Vol. 25, pp. 27-45). https://doi.org/10.1007/978-94-6265-026-8

Mohebbi, D., & Amiri, A. (2025). Legal and Ethical Challenges Related to the Use of Artificial Intelligence in the Administrative Justice System. *Legal Studies in Digital Age*, 1-8.

Nyst, C., & Falchetta, T. (2017). The right to privacy in the digital age. *Journal of Human Rights Practice*, *9*(1), 104-118. https://doi.org/10.1093/jhuman/huw026

Poscher, R. (2021). Artificial intelligence and the right to data protection. In (pp. 281-289). https://doi.org/10.1017/9781009207898.022

Rajaei, M., & Amiri, A. (2024). Principles Governing the Use of Artificial Intelligence in the Realization of Administrative Justice. *Interdisciplinary Studies in Society, Law, and Politics*, *4*(4), 1-8. https://doi.org/10.61838/kman.isslp.4.4.5

Rajaei, M., & Amiri, A. (2025). Rereading Islamic Principles in Supporting Citizens' Economic Rights in the Face of Budget Deficits. *Strategic Studies of Jurisprudence and Law*, e224783. https://doi.org/10.22034/ejs.2025.506231.2037

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data Privacy and Protection: Legal and Ethical Challenges. In *Emerging Threats and Countermeasures in Cybersecurity* (pp. 433-465). https://doi.org/10.1002/9781394230600.ch19

Rostovska, K., Hryshyna, N., Pakhomova, I., Liubchyk, V., & Koval, M. (2024). Place of Principles of Law in Legal Regulation of Public Relations in Conditions of Digital Society: Theoretical and Legal Research. *Syariah: Jurnal Hukum dan Pemikiran*, *24*(1), 73-87. https://doi.org/10.18592/sjhp.v24i1.12647

Shaelou, S. L., & Razmetaeva, Y. (2023). Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values. *Era Forum*, *24*(4), 567-587. https://doi.org/10.1007/s12027-023-00777-2

Solove, D. J. (2025). Artificial intelligence and privacy. *Fla. L. Rev.*, *77*, 1. https://doi.org/10.1093/9780197771716.003.0002

Yanamala, A. K. Y., & Suryadevara, S. (2023). Advances in data protection and artificial intelligence: Trends and challenges. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), 294-319.

Zuwanda, Z. S., Lubis, A. F., Solapari, N., Sakmaf, M. S., & Triyantoro, A. (2024). Ethical and Legal Analysis of Artificial Intelligence Systems in Law Enforcement with a Study of Potential Human Rights Violations in Indonesia. *The Easta Journal Law and Human Rights*, *2*(03), 176-185. https://doi.org/10.58812/eslhr.v2i03.283