ISSN (онлайн): 2663-8959 | ISSN (друк): 2308-6912

УДК 341.231.14:341.3:341.4:004.8
https://doi.org/10.17721/apmv.2026.166.1.49-59

INTERNATIONAL HUMAN RIGHTS LAW AND INTERNATIONAL HUMANITARIAN LAW IN THE ERA OF ARTIFICIAL INTELLIGENCE

МІЖНАРОДНЕ ПРАВО ПРАВ ЛЮДИНИ ТА МІЖНАРОДНЕ ГУМАНІТАРНЕ ПРАВО В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ

Naděžda Šišková
Assoc. Prof. et Assoc. Prof., JUDr., Ph.D (Associated Professor in EU Law and International Law - habilitation and Associated Professor in International Relations - habilitation, Doctor of Law, Ph.D), Head of Jean Monnet Centre of Excellence in EU Law, Faculty of Law Palacký University, President of the Czech Association for European Studies, Editor in Chief of "European Studies. The Review of European Law, Economics and Politics."
E-mail: nadezda.siskova@upol.cz
ORCID ID: https://orcid.org/0000-0001-7019-5032

Maryna Medvedieva
Doctor of Law, Professor at the International Law Chair of the Educational and Scientific Institute of International Relations of Taras Shevchenko National University of Kyiv.
E-mail: medvedieva.maryna@gmail.com
ORCID ID: https://orcid.org/0000-0003-4010-4659

Надєжда Шишкова
Аасоційований професор права ЄС та міжнародного прав (габілітація); асоційований професор міжнародних відносин (габілітація); доктор права, Ph.D., керівниця Центру досконалості Жана Моне з права ЄС, юридичний факультет Університету Палацького; президентка Чеської асоціації європейських студій; головна редакторка журналу «European Studies. The Review of European Law, Economics and Politics».
E-mail: nadezda.siskova@upol.cz
ORCID ID: https://orcid.org/0000-0001-7019-5032

Марина Медведєва
Доктор юридичних наук, професор, професор кафедри міжнародного права Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.
E-mail: medvedieva.maryna@gmail.com
ORCID ID: https://orcid.org/0000-0003-4010-4659

Abstract. *The rapid development and application of artificial intelligence raise fundamental questions for both International Human Rights Law and International Humanitarian Law, particularly regarding accountability, transparency, human control, the protection of fundamental rights, and the principles governing the conduct of warfare. The global regulatory mechanism for AI remains fragmented and underdeveloped, creating legal uncertainty and potential accountability gaps. The purpose of this article is to analyze the main risks AI poses to human rights and to the rules governing armed conflicts, and to consider the main regulatory frameworks in these spheres from an international legal standpoint.*

The authors conclude that there is no single universal treaty governing the protection of human rights in the era of AI. At the universal level, the risks and benefits of AI for human rights have been the subject of reports by various UN bodies, including the Human Rights Council, the Office of the High Commissioner for Human Rights, and UNESCO. The UN General Assembly, UNESCO, and other universal international organizations adopted relevant resolutions and recommendations, but these instruments constitute soft law and do not have binding force. The first legally binding document in the sphere of AI and human rights – the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law – is a regional treaty and has several drawbacks. Although the European Court of Human Rights has dealt with cases related to data protection and digital technologies that may violate the right to privacy, it has not had the opportunity to analyze the direct effects of AI on human rights in those cases. The Artificial Intelligence Act adopted by the European Union is not an instrument specifically addressing human rights. On the other hand, this Regulation

imposes obligations (including sanctions) on AI providers and establishes the structure of implementing and control bodies at the EU and national levels of Member States, which ensure the provision of a safe and ethically healthy environment, thereby creating the preconditions for the protection of human rights.

Lethal autonomous weapon systems that can select and attack targets without human intervention pose serious challenges for International Humanitarian Law. The use of LAWS may breach its main principles: distinction, military necessity, proportionality, precautions in attack, and humanity. The author concludes that there is no single universal treaty governing the conduct of warfare in the era of AI. The UN General Assembly adopted a special resolution on this matter; the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems within the Convention on Certain Conventional Weapons adopted a set of eleven guiding principles, but they constitute soft law and do not have binding force for states. Meanwhile, some organizations called for a new international treaty that would set out specific prohibitions and restrictions on LAWS. It is a matter for future negotiations between states and within international organizations on whether to adopt a new legally binding instrument on such weapons and, if so, in what form. In any case, the current legal framework – conventions and protocols, which are the main sources of International Humanitarian Law – is not enough to govern new weapons developed through AI technologies.

***Keywords**: artificial intelligence, international law, human rights, lethal autonomous weapon systems, international human rights law, international humanitarian law.*

***Анотація.** Стрімка розробка та використання штучного інтелекту порушує фундаментальні питання як для міжнародного права прав людини, так і для міжнародного гуманітарного права, зокрема щодо відповідальності, прозорості, людського контролю та захисту основоположних прав, а також принципів, що регулюють ведення війни. Глобальний механізм регулювання у сфері ШІ залишається фрагментованим і недостатньо розвиненим, що створює правову невизначеність і потенційні прогалини у притягненні до відповідальності. Метою цієї статті є аналіз основних ризиків, які ШІ становить для прав людини та для норм, що регулюють збройні конфлікти, а також розглянути ключові регуляторні рамки у цих сферах з точки зору міжнародного права.*

Автори доходять висновку, що не існує єдиного універсального договору, який би регулював захист прав людини в епоху ШІ. На універсальному рівні ризики та переваги ШІ для прав людини були предметом доповідей різних органів ООН, зокрема Ради ООН з прав людини, Управління Верховного комісара ООН з прав людини та ЮНЕСКО. Генеральна Асамблея ООН, ЮНЕСКО та інші універсальні міжнародні організації відповідні резолюцій і рекомендацій, однак ці інструменти мають характер «м'якого права» і не є юридично обов'язковими. Перший юридично обов'язковий документ у сфері ШІ та прав людини – Рамкова конвенція про штучний інтелект, права людини, демократію та верховенство права – є регіональним договором і має низку недоліків. Хоча Європейський суд з прав людини розглядав справи, пов'язані із захистом даних і цифровими технологіями, які можуть порушувати право на приватність, він не мав можливості проаналізувати безпосередній вплив ШІ на права людини у цих справах. Акт Європейського Союзу про штучний інтелект не є інструментом, спеціально спрямованим на захист прав людини. З іншого боку, цей Регламент покладає обов'язки (включно із санкціями) на постачальників систем штучного інтелекту та встановлює структуру органів імплементації й контролю на рівні ЄС і національному рівні держав-членів, які забезпечують створення безпечного та етично здорового середовища, тим самим формуючи передумови для захисту прав людини.

Летальні автономні системи озброєння, здатні обирати та уражати цілі без втручання людини, становлять серйозні виклики для міжнародного гуманітарного права. Використання таких систем може порушувати його основні принципи: розрізнення, військової необхідності, пропорційності, застосування запобіжних заходів під час нападу та гуманності. Автор доходить висновку, що не існує єдиного універсального договору, який би регулював ведення війни в епоху ШІ. Генеральна Асамблея ООН ухвалила спеціальну резолюцію з цього питання; Група урядових експертів з новітніх технологій у сфері летальних автономних систем

озброєння в рамках Конвенції про певні види звичайної зброї ухвалила одинадцять керівних принципів, однак вони мають характер «м'якого права» і не є юридично обов'язковими для держав. Водночас деякі організації закликали до укладення нового міжнародного договору, який би встановлював конкретні заборони та обмеження щодо такої новітньої зброї. Питання про те, чи буде ухвалено новий юридично обов'язковий міжнародний інструмент щодо летальних автономних систем озброєння і в якій формі, є предметом майбутніх переговорів між державами та в межах міжнародних організацій. У будь-якому разі чинна правова база – конвенції та протоколи, які є основними джерелами міжнародного гуманітарного права, – є недостатньою для регулювання нових видів озброєнь, розроблених із використанням технологій штучного інтелекту.

***Ключові слова**: штучний інтелект, міжнародне право, права людини, летальні автономні системи озброєнь, міжнародне право прав людини, міжнародне гуманітарне право.*

Introduction. The rapid integration of artificial intelligence (hereinafter – AI) into military, law enforcement, administrative, and surveillance systems is profoundly transforming the way power is exercised by states and non-state actors. These technological developments raise fundamental questions for both International Human Rights Law and International Humanitarian Law, particularly regarding accountability, transparency, human control, and the protection of fundamental rights and the principles governing the conduct of warfare. As AI systems increasingly influence decisions affecting life, liberty, privacy, and bodily integrity, existing legal frameworks are being tested in unprecedented ways. The relevance of this topic is further underscored by the growing use of AI in armed conflict, including in targeting, intelligence analysis, autonomous and semi-autonomous weapons systems, and information operations. These developments challenge core International Humanitarian Law principles, such as distinction, proportionality, and precaution, while also raising concerns under International Human Rights Law regarding the right to life, due process, non-discrimination, and the right to effective remedies. The interaction between these two branches of modern International Law in AI-enabled contexts, therefore, requires renewed doctrinal and practical analysis.

Moreover, the global regulatory mechanism for AI remains fragmented and underdeveloped, creating legal uncertainty and potential accountability gaps. Scholarly examination of how existing international legal norms apply to AI technologies is essential to ensure that technological innovation does not outpace legal safeguards. This topic is thus highly relevant to advancing legal certainty, protecting human dignity, and developing responsible governance frameworks for AI in both peacetime and armed conflict.

The purpose of the study. The purpose of this article is to analyze the main risks AI poses to human rights and the rules governing armed conflicts, and to consider the main regulatory frameworks in these spheres from an international legal standpoint.

Literature review. To conduct thorough research on the stated problem, we used the papers of various foreign authors. There are some scientific works dedicated to the issue of the regulation of AI by International Human Rights Law (Balcerzak M., Druzin B., Boute A., Ramsden M., Dulka A., Fowowe A.I., Gellers J.C., Gunkel D., Leslie D., Burr Ch., Aitken Mh., Cowls J., Katell M., Briggs M., McGregor L., Murray D., Ng V., Morawska E.H., Tu X., de Castro e Silva B., Craig, P., De Búrca, G., Hogan, L., Lasek-Markey, M.) as well as by International Humanitarian and Criminal Law (Badhan D., Jagota R., Davison N., Humble K., Nasu H., Ojha Y., Perrin B., Szpak A.). We used these works in the current paper to outline the main issues regarding the relationships between AI technologies and International Law in the spheres of human rights and armed conflicts. Unlike the majority of scientific research on these topics, we analysed the full spectrum of major problems related to the regulation of AI technologies under International Human Rights Law, International Humanitarian Law, and International Criminal Law.

Main results of the research. The first area of concern is the effect of AI technologies on human rights. The protection of human rights and human dignity in the face of technological innovations pertains to the so-called 'fourth generation' of human rights (*Gellers, & Gunkel, 2023*). Although AI

offers numerous benefits for humans and their rights, it also poses significant risks. Here, we provide just a few such examples. First, there may be cases where a system is filled with biased information, leading to algorithmic discrimination that affects certain vulnerable groups. In addition, when forecasting is carried out using AI, the relevant algorithms may fail to account for discriminatory factors (such as gender, age, and ethnicity) and thus may reinforce existing injustices or create new ones (*Leslie et al., 2021*). Second, the gathering, handling, evaluation, and application of users' biometric, behavioural, and genetic information may lead to the risk of constant and intrusive monitoring, creating serious dangers for privacy and data protection, as the highly sensitive and individualized data involved may allow individuals' most private aspects to be disclosed, misused, or otherwise exploited (*Tu, & de Castro e Silva, 2025*). Third, the rapid integration of artificial intelligence into criminal justice systems across numerous countries, particularly through tools designed to evaluate risk and predict the probability of criminal activity by individuals or in specific locations, offers notable operational benefits while simultaneously raising serious concerns about potential infringements on personal freedom and the right to individual liberty (*Fowowe, 2021*). Also, judicial decisions supported or informed by AI may negatively affect the judiciary's rulemaking and decisional independence (*Leslie et al., 2021, p. 15)*.

Due to the potential risks and possible harm to human rights and even some threat to the whole humankind posed by AI, some scholars argue that there is an international legal obligation on states under the right to life within international human rights law to proactively take regulatory action to mitigate the potential existential risk of AI, based on the precautionary principle (*Druzin, Boute, & Ramsden, 2025*). The principle holds that, in situations with the potential for significant harm, even in the absence of full scientific certainty, preventive measures should not be postponed if delayed action may result in irreversible consequences (*Druzin, Boute, & Ramsden, 2025*). Such measures may include, *inter alia*: (1) adoption of *ex ante* regulation, when states may introduce binding legal frameworks that regulate AI systems before their deployment, especially if such systems may pose a certain risk for human rights in some sensitive areas; (2) adoption of moratoria or bans, when risks to human rights are particularly serious or irreversible; (3) elaboration of Human Rights Impact Assessment mechanism which are usually enforced before the deployment of AI; (4) creation of independent oversight bodies to audit the impacts of AI on human rights and intervene where risks emerge; (5) development of the accountability schems and remedies which help the victims of human rights violations to access to complaint mechanisms, judicial or administrative remedies, and enforce their right to challenge AI-based decisions.

Other authors, like Dulka A., proposed some frameworks to regulate AI in relation to human rights, namely: (1) areas where AI can be used with little concern; (2) areas where AI can be used with appropriate measures of caution and constraint; (3) high risk areas where the major costs might still be outweighed by the potential benefits; and (4) areas where the use of AI is never appropriate and must be prohibited by national and international law (*Dulka, 2023*). In this last sense, there must be some 'red lines' which can't be overcome, and law is to become a safeguard in relation to such prohibited spheres which infringe fundamental human rights and undermine the very concept of human dignity. For example, a state may prohibit decisions made exclusively on the basis of an algorithm, without the possibility of human intervention (*McGregor, Murray, & Ng, 2019, p. 337*).

Under international human rights law, states are required to establish preventive legal and institutional structures, ensure supervision and control, impose responsibility for violations, and guarantee effective remedies, while also – through the doctrine of due diligence – obliging public authorities to shield individuals and communities from rights-related harms caused not only by state conduct but also by private actors, including commercial entities (*McGregor, Murray, & Ng, 2019, p. 311-312*). This rule applies to all activities within a state's jurisdiction or under its control related to the use of AI.

At the universal level, the risks and benefits of AI for human rights have been the subject of reports by various UN bodies, including the Human Rights Council, the Office of the High Commissioner for Human Rights, and UNESCO (*Balcerzak, 2024, p. 7-15*). The UN General Assembly Resolution A/78/L.49 'Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development' (2024) emphasizes that human rights and

fundamental freedoms must be respected, protected and promoted throughout the life cycle of artificial intelligence systems, and calls upon all Member States and other stakeholders to refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law (*The UN General Assembly. Resolution A/78/L.49*). UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) refers to some basic fundamental values of the International Human Rights Law, namely safety, non-discrimination, sustainability, right to privacy and data protection, transparency, etc. (*UNESCO. Recommendation*). Some monitoring treaty bodies of the UN system issued a number of general comments, e.g., General Recommendation No. 36 (2020) of the Committee on the Elimination of Racial Discrimination on preventing and combating racial profiling by law enforcement officials, which refers to the risk of algorithmic biases (*Balcerzak, 2024, p. 16*).

One of the first legally binding documents in the sphere of AI and human rights – the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law – was adopted in 2024 within the Council of Europe. Negotiators considered several options for such a regional instrument: from a new additional protocol to the European Convention on Human Rights, or amending other Council of Europe treaties (like the Budapest Convention on Cybercrime or Revised Convention for Data Protection) to a non-binding legal act (*Leslie, et al., 2021, p. 27-29*). The Framework Convention relies on other human rights documents, which are of a general nature (the Universal Declaration of Human Rights, and the European Convention on Human Rights) as well as more specific ones (like the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its protocols). The Convention outlines general obligations of states, including the protection of human rights, the integrity of democratic processes, and respect for the rule of law. It also stipulates specific principles governing activities throughout the lifecycle of artificial intelligence systems.

This Convention, unlike the EU Artificial Intelligence Act, primarily applies to the public sector. The application of its rules to the private sector is within the discretion of states. Another prominent feature of the instrument is that matters relating to national defence fall outside its scope. The exclusion of 'national defence or national security' is justified based on Article 1(d) of the Statute of the Council of Europe, according to which, '[m]atters relating to national defence do not fall within the competence of the Council of Europe' (*Morawska, 2024, p. 41*). We should note that, according to the case law of the European Court of Human Rights (hereinafter – ECHR), a state may restrict certain human rights on grounds of national security, but it must strike a fair balance between the two; furthermore, its margin of appreciation will be very limited in this case.

The ECHR has dealt with a number of cases related to data protection and digital technologies that may violate the right to privacy, but most do not concern AI as such. For example, *Glukhin v. Russia* (2023) concerned the use of facial recognition technology and mass video surveillance by the Russian authorities (*European Court of Human Rights, 2025, p. 10*). Though such systems often rely on algorithmic and AI-based processing, however, the Court did not analyse AI as a separate legal category. It ruled that the state had breached the rights to respect for private life and to freedom of assembly. In other cases, the Court addressed algorithmic, automated, and data-driven technologies, particularly in the contexts of surveillance, biometric identification, and large-scale data processing: *S. and Marper v. the United Kingdom* (2008), *Catt v. the United Kingdom* (2019), *Breyer v. Germany* (2020), *Big Brother Watch and Others v. the United Kingdom* (2021). Thus, the ECHR has not had the opportunity to analyze the effects of AI on human rights in its case law directly.

The Artificial Intelligence Act adopted by the European Union in 2024 is not an instrument specifically addressing human rights, though it refers to ensuring a high level of fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union, including the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, the right to non-discrimination, the right to education, consumer protection, workers' rights, the rights of persons with disabilities, gender equality, intellectual property rights, the right to an effective remedy and to a fair trial, the right of defence and the presumption of innocence, the right to good administration and the rights of children (*Regulation (EU)*). It acknowledges that AI may pose risks and infringe fundamental rights protected

by Union law (*Regulation (EU)*). The Act provides that any regulatory framework for AI must be developed in accordance with EU values, the fundamental rights and freedoms, and that AI technology should be human-centric (*Regulation (EU)*). The Act is considered complementary to other EU legislation on data protection, consumer protection, fundamental rights, employment, protection of workers, and product safety (*Regulation (EU)*).

Despite the fact that EU Artificial Intelligence Act has met with a number of critical reactions both from the side of academia, as well as from the side of NGOs (mostly due its rife loopholes), it is necessary to bear in mind that it is a first attempt to regulate the operation of the AI and to limit its intervention into the different spheres, including the field of human rights. Hogan L. stresses: "As the first legislative framework globally to impose outright prohibitions on the specific AI applications deemed incompatible with fundamental rights and EU values, it establishes a significant precedent" (*Hogan, 2024, p. 10*). The Act classifies the risk under certain categories (unacceptable risk, high risk, limited risk, and minimal risk) and determines the level of the posed threats, including those that are related to fundamental rights. The Regulation states *expressis verbis* that its norms are not applicable for AI systems used for military and national security purposes or pure scientific research and development (Art. 2.3 and Art. 2.6) (*Regulation (EU)*).

To the advantages of this instrument undoubtedly belongs the fact that it establishes its own institutional structure of different bodies on the European and national level of the Member States, which should support the implementation and enforcement of the provisions of the Act. The mentioned implementation and control mechanism is supplemented by substantial penalties, which ensure that the provisions of the Regulation will not be "toothless" and that the norms of the Act will be duly respected. The same refers to the chosen legal form of this instrument, which was adopted as a regulation, in other words, as an act, which under its own nature should be binding in its entirety and directly applicable in all Member States of the Union (*Craig, & De Búrca, p. 139-140*).

In contrast to this Regulation, another relevant EU document, European Declaration on Digital Rights and Principles for the Digital Decade (2023) (*European Declaration*) is focused exclusively on the area of fundamental rights, which stems from the digital transformation, including the usage of Artificial Intelligence. Especially Article 8 states that: "Artificial intelligence should serve as a tool for people, with the ultimate aim of increasing human well-being" and formulates the principle that during the usage of AI it is necessary to: "e) providing for safeguards and taking appropriate action, including by promoting trustworthy standards, to ensure that artificial intelligence and digital systems are, at all times, safe and used in full respect for fundamental rights; f) taking measures to ensure that research in artificial intelligence respects the highest ethical standards and relevant EU law" (Art. 9) (*European Declaration*).

Despite the fact that this document, as a political declaration, currently has no legal effect, it nevertheless has great potential and capacity to become, in the future, a nucleus for a binding catalogue of Digital Rights and thus to follow the destiny of the Charter of Fundamental Rights of the EU. If so, some of the improvements are necessary, including the widening of the list of digital rights (*Šišková, 2024, p. 59*) and the introduction of its own control and enforcement mechanisms. In all the cases, it can serve as one of the sources of inspiration for the global regulation of human rights in the age of Artificial Intelligence.

Another area of concern is the application of so-called lethal autonomous weapon systems (hereinafter – LAWS) developed with the help of AI in armed conflicts. There are several definitions of the LAWS provided by expert reports, scientific literature, and documents of international organizations. For example, Davison N. stipulates that an autonomous weapon system is 'any weapon system with autonomy in its critical functions – that is, a weapon system that can select (search for, detect, identify, track or select) and attack (use force against, neutralize, damage or destroy) targets without human intervention' (*Davison, 2017, p. 5*). In its position paper, the International Committee of the Red Cross argues that 'Autonomous weapon systems select and apply force to targets without human intervention. After initial activation or launch by a person, an autonomous weapon system self-initiates or triggers a strike in response to information from the environment received through sensors and on the basis of a generalized "target profile". This means that the user does not choose, or even know, the specific target(s) and the precise timing and/or location of the resulting

application(s) of force' (*ICRC position*). Some authors differentiate between remotely operated and autonomous unmanned vehicles: remotely operated vehicles, as such, usually do not pose challenges for International Law; by contrast, autonomous weapons raise particular difficulties when it comes to making nuanced, context-dependent judgments (*Ojha, 2025, p. 39*).

LAWS pose serious challenges for both International Human Rights Law and International Humanitarian Law. The scientific literature highlights the following key risks. First, autonomous weapons are likely unable to properly determine a person's status (combatant, civilian, *hors de combat*), to classify an object as civilian or military, to assess whether an 'attack' at a given moment is necessary to achieve a military advantage, and whether such an advantage outweighs the damage inflicted in the course of the attack on civilians and civilian objects. Thus, the use of LAWS may breach the main principles of International Humanitarian Law: distinction, military necessity, proportionality, precautions in attack, and humanity. Second, there is uncertainty about who will be responsible – individuals or the state – for violations of International Humanitarian Law resulting from the improper use of LAWS. Third, there is always the possibility of the misuse of the LAWS by terrorists, the integration of LAWS into weapons of mass destruction delivery systems, or unauthorized interference with algorithms or command-and-control systems. That's why additional mechanisms of International Criminal law must be applied in order to combat relevant crimes.

A certain level of human control and involvement in the operation of autonomous weapons is essential for attributing individual criminal responsibility for war crimes and for determining the international responsibility of states for internationally wrongful acts. Key components of human control encompass, among other factors, the foreseeability and dependability of the weapons system in its intended operational context; the capacity for human operators to intervene at all stages of the system's lifecycle, including development, activation, and actual use; sufficient knowledge and information regarding the weapon's capabilities and the environment in which it is deployed; and accountability for actions performed by the autonomous system. Human control must be present during every stage of the application of LAWS: during its development, deployment, and use.

Some authors argue that if a lethal autonomous weapons system perpetrates a war crime, for example, launching an indiscriminate attack within the meaning of Article 8(2)(b)(iv) of the Rome Statute, the question of criminal attribution becomes highly contested (*Badhan, & Jagota, 2025, p. 84-85*). Responsibility may potentially rest with various actors, including the software developer who created the algorithm, the military commander who authorized or deployed the system, or the manufacturer involved in its production (*Badhan, & Jagota, 2025, p. 84-85*). Individuals who design or deploy LAWS may lack the knowledge or intent for criminal responsibility where the system independently selects and engages targets after activation; however, responsibility would clearly arise where a programmer deliberately codes the system to operate contrary to International Humanitarian Law or where a commander deploys a weapon that is inherently incapable of lawful use in the given operational context. It must be noted that, under the Policy on Cyber-Enabled Crimes of the Rome Statute (2025), the Office of the Prosecutor considers that any decision to deploy or use AI technologies must comply with existing obligations under International Humanitarian Law and International Human Rights Law (*Office of the Prosecutor, 2025, p. 15*).

Under the general rules of international law on state responsibility, a state may incur responsibility for the breaches of International Humanitarian Law committed by its armed forces through the use of autonomous weapon systems. Besides, under Article 36 of the Additional Protocol I to the Geneva Conventions, 'in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party' (*Protocol Additional*). Thus, a state will be held responsible if an LAWS is deployed without having undergone sufficient testing or legal review in advance. Nonetheless, some authors underline the problem of the possibility of applying this provision to weapons developed with AI. For example, Nasu H. stipulates that given the dual-use nature of AI technology, many applications of AI may not qualify as 'weapons' or 'means of warfare' for the purpose of this legal review obligation (*Nasu, 2019, p. 11*).

Bearing the above mentioned difficulties in mind, different scholars have proposed alternative

approaches to accountability for LAWS: (1) a **strict liability** model, under which states or manufacturers would be held accountable for failures or malfunctions of such systems, without requiring proof of intent; (2) a **distributed responsibility** framework that allocates legal responsibility among multiple participants according to their involvement at different stages of the autonomous weapons system's lifecycle (*Badhan, & Jagota, 2025, p. 85*).

It must be noted that under the current framework of International Humanitarian Law, the use of some LAWS is to be prohibited completely, namely in situations where such systems cannot meet core requirements of customary and treaty rules of International Humanitarian Law, such as distinction, proportionality, and precaution; where their design renders them inherently indiscriminate or likely to inflict superfluous injury or unnecessary suffering; or where they are directed against civilians or civilian objects (*Perrin, 2025*). Prohibition must also be imposed where their effects cannot be reasonably predicted or controlled, where they operate without sufficient human oversight or judgment in light of the specific context, or where their deployment is intended or foreseeably leads to widespread, long-term, and severe damage to the natural environment (*Perrin, 2025*).

In December 2024, the UN General Assembly adopted resolution A/RES/79/62 called 'Lethal autonomous weapons systems', which encouraged states and international organizations to participate in the work of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (*The UN General Assembly. Resolution A/RES/79/62*). This resolution refers to the initiative being realized within the Convention on Certain Conventional Weapons. At an informal meeting of the High Contracting Parties to the Convention in 2013, the Group of Governmental Experts was granted an open-ended mandate to develop an operational and normative framework governing the use of emerging technologies in LAWS (*Humble, 2023*). This process ultimately led, in 2019, to the Group's set of eleven guiding principles addressing the development, deployment, and use of such systems (*Humble, 2023*).

The principles reaffirm the full applicability of International Humanitarian Law to all weapons and stress the necessity of maintaining meaningful human responsibility and control throughout the entire life cycle of such systems. They emphasize states' obligations to ensure accountability, conduct legal reviews of new weapons, and integrate risk assessment, security, and safeguard measures into the development and deployment of new weapons, including LAWS. The principles caution against anthropomorphizing autonomous systems and underscore the need to balance military necessity with humanitarian considerations. It should be emphasized in this regard that weapons are merely material tools and lack legal personality or independent agency; International Humanitarian Law assigns rights and duties to states and individuals, not to technological systems; accordingly, describing LAWS using concepts such as 'autonomy', 'intelligence', 'self-awareness', or 'decision-making' risks creating a misleading impression about their actual nature and capacities (*Szpak, 2024, p. 290*).

Meanwhile, the United Nations Secretary-General and the President of the International Committee of the Red Cross called for a new international treaty that would set out specific prohibitions and restrictions on LAWS (*Perrin, 2025*). Many states proposed a moratorium on the use of all LAWS or a ban on their use; however, the Group of Governmental Experts indicates a need to adopt regulations that determine the rules under which LAWS may be legally used, rather than imposing a ban (*Szpak, 2024, p. 292*). It is a matter for future negotiations between states and within international organizations to decide whether to adopt a new legally binding instrument on LAWS and in what form (for example, as a separate convention or an additional protocol to the Convention on Certain Conventional Weapons).

Conclusions. AI offers numerous benefits for humans and their rights; meanwhile, it also poses significant risks. Due to the potential risks and possible harm to human rights (such as the right to privacy, fair trial, freedom from discrimination, etc.) and even some threat to the whole humankind posed by AI, some scholars argue that there is an international legal obligation on states under the right to life within international human rights law to proactively take regulatory action to mitigate the potential existential risk of AI based on the precautionary principle. In any case, there must be some 'red lines' which can't be overcome, and the law is to become a safeguard in relation to such prohibited spheres which infringe fundamental human rights and undermine the very concept of human dignity. Under International Human Rights Law, states are required to establish preventive

legal and institutional structures, ensure supervision and control, impose responsibility for violations, and guarantee effective remedies for any harm inflicted by the use of AI technologies.

There is no single universal treaty governing the protection of human rights in the era of AI. At the universal level, the risks and benefits of AI for human rights have been the subject of reports by various UN bodies, including the Human Rights Council, the Office of the High Commissioner for Human Rights, and UNESCO. The UN General Assembly, UNESCO, and other universal international organizations adopted some resolutions and recommendations, but these instruments constitute soft law and do not have binding force. The first legally binding document in the sphere of AI and human rights – the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law – is a regional treaty and has several drawbacks, namely, it primarily applies to the public sector and doesn't address the matters relating to national defence. Although the European Court of Human Rights has dealt with cases related to data protection and digital technologies that may violate the right to privacy, it has not had the opportunity to analyze the direct effects of AI on human rights in those cases.

The Artificial Intelligence Act adopted by the European Union belongs to secondary legislation of the EU and is not an instrument specifically addressing human rights. On the other hand, this Regulation imposes obligations (including sanctions) on AI providers and establishes the structure of implementing and control bodies at the EU and national levels of Member States, which ensure the provision of a safe and ethically healthy environment, thereby creating the preconditions for the protection of human rights. As such, its norms could partly serve as a certain model for the global regulation of these matters. Another EU document, the European Declaration on Digital Rights and Principles (2023), is focused directly on the human rights area; nevertheless, due to its non-binding character, it cannot protect the rights of individuals but could be used as a source of inspiration for the regulation of these issues at the level of International Law.

Lethal autonomous weapon systems that can select and attack targets without human intervention pose serious challenges for International Humanitarian Law. The use of LAWS may breach its main principles: distinction, military necessity, proportionality, precautions in attack, and humanity. A certain level of human control and involvement in the operation of autonomous weapons is essential for attributing individual criminal responsibility for war crimes and for determining the international responsibility of states for internationally wrongful acts. Responsibility may potentially rest with various actors, including the software developer who created the algorithm, the military commander who authorized or deployed the system, the manufacturer involved in its production, and the state itself. Under the general rules of international law on state responsibility, a state may incur responsibility for the breaches of International Humanitarian Law committed by its armed forces through the use of autonomous weapon systems, as well as for the use of LAWS deployed without having undergone sufficient testing or legal review in advance. Under the current framework of International Humanitarian Law, the use of some LAWS is to be prohibited completely, namely in situations where such systems cannot meet core requirements of customary and treaty rules of International Humanitarian Law.

There is no single universal treaty governing the conduct of warfare in the era of AI. The UN General Assembly adopted a special resolution on this matter; the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems within the Convention on Certain Conventional Weapons adopted a set of eleven guiding principles, but they constitute soft law and do not have binding force for states. Meanwhile, the United Nations Secretary-General and the President of the International Committee of the Red Cross called for a new international treaty setting out specific prohibitions and restrictions on LAWS. It is a matter for future negotiations between states and within international organizations to decide whether to adopt a new legally binding instrument on LAWS and in what form (for example, as a separate convention or an additional protocol to the Convention on Certain Conventional Weapons). In any case, the current legal framework – conventions and protocols, which are the main sources of International Humanitarian Law – is not sufficient to govern new weapons developed through AI technologies, and the new globally recognized rules, including the effective control mechanism, must be urgently elaborated. This appeal is extremely pressing, especially in the light of Russian aggression against

Ukraine and the deterioration of the entire political and security climate in the world.

Funding: *no external funding.*
Conflict of Interest: *the authors declare no conflict of interest regarding the publication of this article.*
Data Availability Statement: *not applicable*

References:

Badhan, D., & Jagota, R. (2025). Emerging technologies in warfare: Legal challenges for international criminal jurisprudence. *International Journal of Law*, 11(5), 84-89.

Balcerzak, M. (2024). Implications of the United Nations human rights standards for the development of artificial intelligence. In M. Balcerzak & J. Kapelańska-Pręgowska (Eds.), *Artificial Intelligence and International Human Rights Law: Developing Standards for a Changing World* (pp. 6-24). Cheltenham, UK: Edward Elgar Publishing.

Craig, P., & De Búrca, G. (2020). *EU Law: Text, Cases and Materials* (8th ed.). Oxford: Oxford University Press.

Davison, N. (2017). A legal perspective: Autonomous weapon systems under international humanitarian law. *UNODA Occasional Papers: Perspectives on Lethal Autonomous Weapon Systems,* 30, 5-18.

Druzin, B., Boute, A., & Ramsden, M. (2025). Confronting Catastrophic Risk: The International Obligation to Regulate Artificial Intelligence. *Michigan Journal of International Law*, 46(2), 173-217.

Dulka, A. (2023). The Use of Artificial Intelligence in International Human Rights Law. *Stanford Technology Law Review*, 26(2), 316-366.

European Court of Human Rights. (2025). *Judicial Seminar 'Protecting human rights in a world of Artificial Intelligence, algorithms and big data'. Background Document*. Retrieved from https://www.echr.coe.int/documents/d/echr/seminar-background-paper-2025-eng.

European Declaration on Digital Rights and Principles for the Digital Decade, 2023. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023C0123(01).

Fowowe, A.I. (2021). *Artificial Intelligence and Human Rights*. Retrieved from https://ssrn.com/abstract=3964199.

Gellers, J.C., & Gunkel, D. (2023). Artificial Intelligence and International Human Rights Law: Implications for Humans and Technology in the 21st Century and Beyond. In A. Zwitter & O. Gstrein (Eds.), *Handbook on the Politics and Governance of Big Data and Artificial Intelligence* (pp. 430-455). Cheltenham, UK: Edward Elgar Publishing.

Hogan, L., & Lasek-Markey, M. (2024). Towards a Human Rights-Based Approach to Ethical AI Governance in Europe. *Philosophies*, 9(6), Retrieved from https://www.mdpi.com/2409-9287/9/6/181.

Humble, K. (2023). Artificial intelligence and the need for an international legal framework in the race for killer robots in modern warfare. In A. Završnik & K. Simončič (Eds.), ***Artificial Intelligence, International Law and Social Harms*** (pp. **57-77**). Cham: Palgrave Macmillan.

ICRC position on autonomous weapon systems. (2021). Retrieved from https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

Leslie, D., Burr, Ch., Aitken, Mh., Cowls, J., Katell, M., & Briggs, M. (2021). *Artificial intelligence, human rights, democracy, and the rule of law: a primer*. The Council of Europe.

McGregor, L., Murray, D., & Ng, V. (2019). International Human Rights Law as a Framework for Algorithmic Accountability. *International and Comparative Law Quarterly*, 68, 309-343.

Morawska, E.H. (2024). Council of Europe standards and activities related to AI: towards a Framework Convention on AI and human rights? In M. Balcerzak & J. Kapelańska-Pręgowska (Eds.), *Artificial Intelligence and International Human Rights Law: Developing Standards for a Changing World* (pp. 25-44). Cheltenham, UK: Edward Elgar Publishing.

Nasu, H. (2019). Artificial Intelligence and the Obligation to Respect and to Ensure Respect for International Humanitarian Law. *ECIL Working Paper 2019/3*. Retrieved from

https://www.exeter.ac.uk/v8media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Nasu_-_AI_and_IHL_-_ECIL_WP_2019-3.pdf.

Office of the Prosecutor. (2025). *Rome Statute Policy on Cyber-Enabled Crimes under the Rome Statute*. Retrieved from https://www.icc-cpi.int/sites/default/files/2025-12/2025-cyber-eng.pdf.

Ojha, Y. (2025). Artificial Intelligence in Armed Conflict: Perspectives from International Humanitarian Law. *Unity Journal*, 6, 34-47.

Perrin, B. (2025). Lethal Autonomous Weapons Systems and International Law: Growing Momentum Towards a New International Treaty. *ASIL Insights*, 29(1). Retrieved from https://www.asil.org/insights/volume/29/issue/1.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

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).

Šišková, N. (Ed.). (2024). *Legal Issues of Digitalisation, Robotisation and Cyber Security in the Light of EU Law*. Alphen aan Rijn: Kluwer Law International.

Szpak, A. (2024). Artificial intelligence and international humanitarian law in the work of the parties to the Conventional Weapons Convention: lethal autonomous weapons. In M. Balcerzak & J. Kapelańska-Pręgowska (Eds.), ***Artificial Intelligence and International Human Rights Law*** (pp. **278-293**). Cheltenham, UK: Edward Elgar Publishing.

The UN General Assembly. Resolution A/78/L.49 'Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development'. (2024).

The UN General Assembly. Resolution A/RES/79/62 'Lethal autonomous weapons systems'. (2024).

Tu, X., & de Castro e Silva, B. (2025). Are We Ready for the Metaverse? Implications, Legal Landscape, and Recommendations for Responsible Development. *Digital Society*, 4(9), 1-27.

UNESCO. Recommendation on the Ethics of Artificial Intelligence (2021).

Received: 02.02.26 / Revised: 16.02.26 / Accepted: 18.03.26 / Published:30.03.26