LEGAL REGULATION: EARTH'S REMOTE SENSING, ARTIFICIAL INTELLIGENCE IN UKRAINIAN CONFLICT

SHYSHKAROV Kostiantyn - PhD in Law researcher Department of Private International Law Educational and Scientific Institute of International Relations Taras Shevchenko National University of Kyiv

ORCID: https://orcid.org/0009-0009-5398-6604

Supervisor: Associate Professor, PhD in Law Victor KALAKURA

(UDC) УДК 341.96

DOI: https://doi.org/10.32782/ep.2024.4.14

Examined the regulatory frameworks that govern the use of Earth observation, artificial intelligence (AI) in the context of the Ukrainian conflict. It considers the legal constraints, privacy concerns, international implications associated with the deployment of satellite imagery and AI for intelligence gathering, civilian protection. It weighs these applications against privacy laws, rights and reviews the applicability of international treaties in regulating these technologies in conflict situations.

Keywords: Remote Sensing, Artificial Intelligence, Ukrainian Conflict, Privacy Law, International Treaties, Private International Law.

Problem statement – the accelerated evolution and implementation of these technologies for surveillance, intelligence, and civilian protection have outpaced the current legal framework, especially for private companies' performance, giving rise to intricate questions concerning privacy, sovereignty, ethical use.

State of Research – the academic literature on the legal implications of Earth observation and AI applications in conflict zones has grown considerably in recent years, particularly in response to the advent of new military technologies, surveillance capabilities. Recent studies have focused on the role of private satellite imagery in conflict intelligence, privacy concerns, and the application of AI in real time analysis, collectively underscoring the urgency of developing regulatory frameworks.

Scientific Novelty of the Study (Objective) – the study's objective is to provide actionable guidance for policymakers, legal practitioners by analysing regulatory gaps, sovereignty issues, enforcement challenges. In doing so, it will contribute original knowledge to the fields of private international law, conflict studies, technology governance.

Materials and Methods of Research – this research employs a combination of doctrinal legal analysis, case study examination, ethical evaluation to gain a comprehensive understanding of the subject matter.

Results of Research – in particular, it identifies shortcomings in the legal frameworks that address issues such as data privacy, the dual use nature of these technologies for civilian, military purposes, challenges to state sovereignty.

Discussion of Results – the discussion proposes a framework for addressing regulatory gaps by integrating specific provisions for conflict specific applications of these technologies. This includes protocols for data protection, guidelines for the deployment of AI in military operations.

A synopsis of the principal content

Ukrainian conflict marked strategic importance of remote sensing technology, particularly in intelligence, surveillance, reconnaissance, ISR, operations. This thesis picks up the question of the use of remote sensing in UA conflict, shows how advances in satellite imagery, synthetic aperture radar, SAR, and geospatial intelligence, GEOINT, have changed the landscape of the conflict (war). The use of remote sensing has proven extremely useful for both military and humanitarian purposes, providing valuable insights into troop movements, assessing infrastructure damage, refugee movement patterns etc. Discussing is about the role of key technologies such as commercial satellite services, drones, high resolution optical systems in monitoring real-time, ASAP, changes on the battlefield and providing important data to various stakeholders.

A significant pressing issue is when using remote sensing is ensuring the security and integrity of data, especially in light of the evolving cyber threat landscape. This article addresses the aforementioned cybersecurity challenges with reference to Delaware Act (U.S.) which emphasizes protecting electronic systems from unauthorized access, establishing protocols for the lawful interception, monitoring of electronic data. Given the volume and sensitivity of information transmitted via satellite, other remote sensing means, the regulatory framework of Delaware law provides valuable insights into protecting these assets from potential destruction, unauthorized distribution, and misuse by adversaries. The article highlights on to examine the ethical implications of remote sensing in conflict war zones, with a particular focus on the balance to be struck between transparency, privacy, security. The advent of remote sensing has introduced a number of opportunities, challenges for international humanitarian law, giving rise to concerns regarding the privacy of civilians and the potential for dual use technology applications. [1]

This article marks the ethical considerations associated with the management, dissemination of remote sensing data, with a particular focus on ensuring compliance with the principles of distinction and proportionality in conflict situations. Furthermore, it examines the implications of third party actors, such as private satellite operators and multinational corporations, for the maintenance of neutrality, data impartiality.

This research highlights the need to implement strong cybersecurity measures and establish comprehensive regulatory frameworks to ensure that sensitive data collected through remote sensing is protected, especially in high risk conflict zones such as Ukraine. The study shows that an integrated approach is needed that combines technological innovation, legal regulation, and ethical oversight to optimize the benefits of remote sensing while minimizing risks. This article calls for further research to develop international standards and guidelines for the use of remote sensing technology in conflict and to ensure that these tools are used responsibly and in accordance with humanitarian principles.

A special threat is the excesses of private companies, as it was, for example, with the shutdown of SpaceX satellites for the needs of the armed forces of Ukraine, what legal risks can be prevented here? Perhaps, existing precedents of English – Saxon law? [2]

Can satellites used for military purposes be considered a legitimate target for the opposing side in a conflict? For example, there are developments of passive «weapons» in space, where small spheres are scattered in orbit as the satellite moves, or a spent space object or satellite is destroyed on purpose, and these fragments hit an active satellite used for military purposes. Is it not time, therefore, to revise the 1967 Outer Space Treaty, which states that space is the heritage of all mankind w/o weapons, nuclear weapons? [3]

In the context of the UA conflict, artificial intelligence has become a crucial tool for the management, interpretation, and regulation of remote sensing data, offering significant advancements but also posing unique legal challenges. The integration of AI into remote sensing technologies enables more effective intelligence gathering while raising concerns about data protection, state sovereignty, ethical use, compliance with international humanitarian law, IHL. This article tries to outline the primary legal roles and implications of AI in remote sensing for the UA conflict: [4]

1. The integration of automated data processing and compliance with international law represents a significant advancement in the field of AI. The application of AI in target veri-

fication and distinction represents a particularly promising avenue of research. The capacity of AI to rapidly analyse, categorise satellite imagery and drone data provides a valuable contribution to military decision making, particularly in the differentiation between military and civilian infrastructure which is a crucial aspect of IHL. The application of AI driven object recognition, categorisation facilitates the assurance that only lawful targets are engaged, thereby aligning operations with the principles of distinction and proportionality set forth in IHL.

Predictive modelling and proportionality assessment. AI models can predict the potential impacts of certain military actions, thereby aiding in assessments of proportionality as required by IHL. For instance, AI can analyse the projected destruction in civilian populated areas, thereby assisting decision makers in mitigating unnecessary harm and ensuring compliance with the principle of humanity.

2. Enhanced Data Privacy and Protection Mechanisms under Cybersecurity Law. The utilisation of encryption and data anonymisation techniques: the application of AI driven encryption algorithms serves to enhance cybersecurity, ensuring the confidentiality and integrity of sensitive data transmitted via remote sensing networks. These protocols are aligned with frameworks such as the Delaware Act, which emphasises robust data protection standards to guard against unauthorised access. This is particularly vital in a conflict setting where cyber threats are prevalent.

Intrusion Detection and Anomaly Monitoring. AI powered cybersecurity systems continuously monitor data flow for irregularities or unauthorised access. These systems support compliance with cybersecurity laws such as the Delaware Act which mandates vigilance over data security and confidentiality. This safeguards against data leaks that could compromise both civilian safety and state security.

3. The concept of data sovereignty and the question of compliance with national, international jurisdictional laws are of great importance in the context of data localisation. The following section will address the challenges associated with jurisdictional issues in this field. The use of AI driven remote sensing data frequently transcends national boundaries, giving rise to legal concerns pertaining to data sovereignty, compliance with both national, international legislation. The capacity of AI to localise data storage and processing facilitates the maintenance of compliance with territorial laws that govern data access and usage. This ensures that sensitive information remains within the confines of authorised jurisdictions.

Cross Border Data Sharing Regulations. AI enables the automated compliance with data sharing laws by filtering, anonymising data shared across borders. This is particularly pertinent in the context of the Ukrainian conflict, where international coalitions require data sharing for the purposes of coordination. Legal restrictions on data transfer must be observed to prevent breaches of national sovereignty.

4. The question of legal accountability and transparency in automated decision making is a significant one. It is necessary to consider the ways in which algorithms can be held accountable for their actions, particularly in the context of target selection. The advent of AI driven target recognition and decision making systems has given rise to a few questions pertaining to the accountability and legal responsibility associated with instances of error or misuse. From a legal standpoint, automated systems are required to operate with transparency, particularly in the context of target selection where errors could potentially result in civilian harm. This necessitates the implementation of frameworks for algorithmic accountability, ensuring that AI outputs can be audited, and that human oversight remains integral.

Compliance with Autonomous Systems Regulations. As remote sensing increasingly utilises AI to automate tasks, including surveillance, threat assessment, adherence to laws regulating autonomous weapons systems becomes vital. These laws mandate a level of human control to prevent AI systems from making life or death decisions without human input, aligning with principles of human accountability in military operations.

5. The objective is to guarantee the ethical utilisation of data in accordance with the tenets of international humanitarian law. This entails a comprehensive examination of the potential dual use applications of data, with a particular

focus on their impact on civilian protection. Remote sensing data, particularly that captured by commercial satellites, frequently contains information that could be utilised for both civilian and military purposes. The role of AI in filtering and anonymising civilian related data is instrumental in ensuring compliance with ethical, legal standards that protect civilian privacy. This is consistent with the ethical principles set out in IHL, thereby reducing the risk of civilian data being exploited or of incidental harm being caused.

Privacy in Conflict Zones. The use of AI in remote sensing gives rise to concerns about privacy, particularly in relation to civilians in conflict zones. Legal frameworks such as the Delaware Act, international privacy laws increasingly require that AI applications protect personal data. AI driven anonymisation and data minimisation processes help to fulfil these requirements, ensuring that only relevant, non identifiable data is retained, used.

6. The interplay between cybersecurity law, AI in data integrity and protection. The question of adherence to cybersecurity protocols Artificial intelligence enhances cybersecurity by automating encryption and enforcing compliance with protocols that prevent unauthorised data access, as required by legislation such as the Delaware Act. In the context of the ongoing conflict in Ukraine where cyber threats are pervasive, AI systems are employed to monitor and protect data integrity, thereby securing sensitive information from potential breaches or exploitation by adversarial actors.

Self Healing Networks for Continuous Compliance. AI enabled self healing systems are capable of detecting and mitigating cyber threats in real time, thereby ensuring continuous compliance with cybersecurity laws. These systems are able to autonomously adjust data flow paths and secure nodes, thus guaranteeing uninterrupted data protection which is of critical importance in remote sensing in conflict scenarios where reliable, protected data is essential for operational decisions.

7. The legal standardisation of artificial intelligence, AI, in data sharing protocols is a crucial aspect of international data sharing and dual use export compliance. Artificial intelligence facilitates the uniform adherence to international legislation that governs the export and dissemination of remote sensing data. To illustrate, AI driven filters guarantee that data with potential military applications is not accessed by unauthorised individuals, thereby aligning with export control laws and international security agreements. [5]

Ethical Data Dissemination Standards. AI facilitates compliance with ethical dissemination standards by monitoring data requests and usage to ensure they comply with international regulations on neutrality and non militarisation in conflict zones. This is of particular importance in the context of the Ukrainian conflict where commercial satellite operators provide data to a range of stakeholders and must navigate complex legal frameworks to maintain impartiality and compliance with international law.

Conclusion

It can be stated that AI plays a pivotal role in the enhancement of remote sensing for the management of conflict. However, the utilisation of AI also gives rise to the necessity for the establishment of a sophisticated legal and ethical framework, the objective of which is to ensure compliance with international humanitarian law, cybersecurity protocols and data sovereignty regulations. The capacity of AI to automate target distinction, safeguard sensitive data, and guarantee accountability is in alignment with legal principles that are of paramount importance in conflict zones such as Ukraine. However, it also gives rise to distinctive legal issues concerning the boundaries of autonomy, the entitlements of states and civilians, and the moral implications of dual purpose data use.

By employing frameworks such as the Delaware Act and evolving international standards, the regulation of AI enhanced remote sensing can be achieved in a manner that secures sensitive data, safeguards civilian privacy, and facilitates lawful military operations. A comprehensive legal approach is vital to optimising the benefits of AI while ensuring ethical and legal compliance in high-stakes contexts.

It is imperative that stringent control be exercised with regard to the collaboration with private military enterprises, as well as the intercompany alliances that they form. This particular area of concern falls within the purview of private international law.

A separate issue is the settlement of geothermal and geological weapons, using the Earth's crust for cataclysms, can such incidents be recognized by satellite? How to make it here that the rules are the force of law, not the right of force? [6][7][8].

List of sources

1. Delaware General Assembly – Delaware Act: https://delcode.delaware.gov/title6/c018/

2. Reuters – SpaceX curbed Ukraine's use of Starlink internet for drones -company president: https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/#:~:text=SpaceX%20has%20taken%20steps%20to%20prevent%20Ukraine%27s%20military,country%27s%20war%20with%20Russia%2C%20SpaceX%27s%20president%20said%20Wednesday.

3. Держави-учасниці цього Договору – Договір про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла: Договір про принципи діяльності держав... | від 27.01.1967 (rada.gov.ua)

4. European Commission – The War in Ukraine and AI Regulation: Some Controversial Takeaways: https://futurium.ec.europa.eu/en/european-ai-alliance/blog/war-ukraine-and-ai-regulation-some-controversial-takeaways

5. Center for a New American Security – Roles and Implications of AI in the Russian-Ukrainian Conflict: https://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict

6. ScienceNews – Geologists develop weapons to combat that sinkhole feeling: https://www.sciencenews.org/article/geologists-develop-weapons-combat-sinkhole-feeling

7. ScienceDirect – Global review of human-induced earthquakes: https://www.sciencedirect.com/science/article/pii/S001282521730003X?via%3Dihub

8. Federation of American Scientists: Address by US Secretary of State at 1997 conference on terrorism

Рассмотрена нормативно-правовая база, регулирующая использование данных наблюдения Земли и искусственного интеллекта (ИИ) в контексте конфликта в Украине. Рассматриваются правовые ограничения, проблемы конфиденциальности, международные последствия, связанные с использованием спутниковых снимков и ИИ для сбора разведданных, защиты гражданского населения. В нем взвешиваются эти приложения с точки зрения законов, прав на неприкосновенность частной жизни и рассматривается применимость международных договоров для регулирования этих технологий в конфликтных ситуациях.

Ключевые слова: дистанционное зондирование, искусственный интеллект, украинский конфликт, право конфиденциальности, международные договоры, международное приватное право.