

The Illusion of Legal Rights: Regulating AI-Powered Satellite Surveillance to Protect Privacy, Sovereignty and Security

Alka Patil¹, Eshan Borikar², Mangala Venkatraman³

¹ University of Mumbai, India

² Advocate, Bombay High Court, Visiting Faculty at Government Law College, Mumbai and University of Mumbai, India

³ Advocate, Kerala High court and former Visiting Faculty at Government Law College, Mumbai and Siddharth Law College, Mumbai, India

ABSTRACT

The rapid proliferation of AI-powered Geo-spatial technologies threatens to devalue privacy, sovereignty, and security into illusory rights. This paper investigates the rapid development of AI-powered satellite surveillance and its legal consequences guided by the following research question: How effective are current legal frameworks in addressing the risks posed by AI-powered geo-spatial surveillance, and what reforms are necessary to protect fundamental rights? The authors have scrutinised key international instruments and domestic statutes, including the Digital Personal Data Protection Act (2023), National Geo-spatial Policy (2022), Information Technology Act, 2000, UN Sustainable Development Goals (SDG 16) and analysed operational AI- satellite systems like SkySat (USA), RISAT-2B (India), Gaofen-7 (China), HawkEye 360 (USA) and Ofek-16 (Israel) for technical diversity.

The authors have employed black-letter and comparative analysis to identify critical gaps in the existing legal and policy frameworks in light of increased international conflicts and covert governmental interventions. The study reveals key findings that the existing legal framework and policy fail to encapsulate dynamic AI-powered technology. Additionally, the paper looks into the roles of the stakeholders, commercial operators, watchdogs and civil society involved in geo-spatial AI satellite surveillance and outlines regulatory measures. To address these challenges, the study proposes a mandatory human rights impact audit, an independent geo-spatial oversight authority and comprehensive legislation to weave the collection of AI-geospatial data harmoniously into the complex web of human rights to keep the people's privacy and the nation's security and sovereignty intact.

Keywords: AI-powered satellite surveillance, privacy, legal framework, human rights, geospatial technology.

1. INTRODUCTION

Once introduced to human society, technological development can neither be withdrawn nor undone. Hence, the only step forward is for the technology to be studied, developed and amalgamated into society in such a manner as to ensure the preservation and protection of human lives and human rights. Geo-spatial technology is a system used to acquire, store, analyse, and output data in two or three dimensions. Geo-spatial technologies (GST) encompass thematic mapping, global positioning systems (GPS), remote sensing (RS), telemetry, and Geographic information systems (GIS) (Philip A. Reed & John Ritz, 2004).

The infinite benefits that AI-powered geo-spatial surveillance data presents in disaster preparedness, environmental protection, economic development and city planning can neither be denied nor overlooked. At the same time, the risks it poses and the threats it presents can also not be ignored. The unbridled proliferation of AI-powered Geo-spatial technologies threatens to devalue privacy, sovereignty and security into illusory rights, thereby calling for an imminent need to evaluate the existing laws and policies and analyse the changes required to match the rise in technology. Operational AI- satellite systems like SkySat (USA), RISAT-2B (India), Gaofen-7 (China), HawkEye 360 (USA) and Ofek-16 (Israel) are key players in the geo-spatial AI surveillance sphere, and they are studied for technical diversity.

The rapid development of AI-powered satellite surveillance and its legal consequences raises the following research question: How effective are current legal frameworks in addressing the risks posed by AI-powered geo-spatial surveillance, and what reforms are necessary to protect fundamental human rights?

The authors identify critical gaps in the existing legal and policy frameworks in light of increased international conflicts and covert governmental interventions. The study reveals key findings that the existing legal framework and policy fail to encapsulate dynamic AI- powered technology. Additionally, the paper looks into the roles of the stakeholders, commercial operators, watchdogs and civil society involved in geo-spatial AI satellite surveillance and outlines regulatory measures.

The Geospatial Technology Spectrum



Source:- <https://agiindia.com/geospatial-industry-overview/>

2. LITERATURE REVIEW

The intersection between artificial intelligence, satellite surveillance, and legal regulation is poignant. The paper explores three fundamental legal theories:(1) technological determinism in law (Winner,1980; Lessig,2006), wherein law evolves with the rapid evolution of technology. The law should not only react but also have future oversight. It shows that technological developments will lead to shaping legal possibilities. (2) privacy as contextual integrity (Nissenbaum,2010) is relevant to overhead surveillance, where

only secrecy is not the objective, but the objective is to secure the right to appropriate information flow. (3) The third most important legal theory is sovereignty in the digital (Johnson& Post, 1996; Goldsmith& Wu,2006) and Artificial Intelligence age. This theory is important to understand that, with rapid technological development, we can protect the state's sovereignty.

2.1. PRIVACY AND SURVEILLANCE

There has been a considerable development in satellite surveillance privacy compared to initial research (Clarke,1988) on satellite surveillance and its implications. There has been a massive commercialisation of space in recent years, so there is an imminent need for regulation. The study of commercial satellites and privacy-related issues (Molnar,2021) highlights the threats. However, it fails to recognise the threats of the new age, especially a shift from human-based to algorithmically processed imagery data.

2.2. LEGAL GAPS

The scholars have focused more on space law regulations governing traditional state-to-state obligations under the Outer Space Treaty (1967) (Hobe et al.,2017; von der Dunk,2015). The recent research by Lyall and Larsen, 2018 highlights the lack of a legal framework for commercial satellites launched by private stakeholders. Our research goes one step ahead and addresses the risk of a serious regulatory gap due to AI-enabled satellite surveillance.

3. METHODOLOGY

3.1. RESEARCH DESIGN

This study will deploy black letter and comparative legal analysis to evaluate the adequacy of the existing rules governing AI-powered satellite surveillance. The primary sources include the treaties, statutes, policy papers, judicial decisions, and secondary literature, such as scholarly commentary and research papers. A technical legal matrix was developed to translate the doctrinal requirements into indicators showing AI-powered satellites' functions.

3.2. SATELLITE SAMPLE AND JUSTIFICATION

The five systems were purposively selected based on ownership, ability and jurisdiction.

Act,2000 (Ministry of Electronics and Information Technology,2000), rules, and policy. At the international level, it has been evaluated through the prism of the Outer Space Treaty, remote sensing principles, and GDPR to show comparative privacy analysis and other necessary policies (Amirfar et al.,2023).

It is clear that appropriate legal regulations do not fill the legal gaps. Legal development is far behind technical innovation in this segment. The study identifies legal obligations and accountability pathways for commercial operators, state agencies, watchdog bodies and civil society. Findings of the study call for a structural legal reform in the system by introducing a mandatory human rights impact audit for AI-powered surveillance satellites in high- resolution missions (European Network of National Human Rights Institutions

(ENNHRI) (n.d.). There is an imminent need to create an independent geo-spatial oversight body to regulate such satellites, coupled with investigation powers.

4.EVALUATION PARAMETERS

4.1. PRIVACY

The study explores the potential intrusion by the AI-powered surveillance satellites into individual and organisational autonomy, in contrast to the Digital Personal Data Protection Act 2023(Ministry of Electronics and Information Technology ,2024) and compares the other data protection regimes.

4.2. SOVEREIGNTY

There is a need to respect India's jurisdictional control over its territory and data. It will evaluate whether it aligns with the National Geo-spatial Policy,2022 (Press Information Bureau,2025), Remote Sensing Data Policy,2011 (National Remote Sensing Centre [NRSC], ISRO 2025) and customary principles like non-appropriation under the Outer Space (TreatyUnited Nations Office for Outer Space Affairs [UNOOSA] (n.d.).

4.3. SECURITY

The study analysed the dual risks, such as the potential of espionage and exposure of critical infrastructure. It considered the parameters such as national security, expert control frameworks, and UN SDG16 guidelines on peace, justice and strong institutions.

5.LEGAL FRAMEWORK

The study relied on an analytical framework to gauge the risks involved in parameters like resolution, revisit, onboard AI functions, and data downlink paths. It has been evaluated through the prism of Indian law, i.e DPDPA Act,2023(Ministry of Electronics and Information Technology [MeitY],2024), Information Technology

5.1. TECHNICAL AND LEGAL MATRIX

We have worked to make a framework to show which laws can regulate these AI-powered satellite surveillance.





Satellite Capabilities, Laws & Violations			
Capability	Law	Violation Example	Severity
 Resolution	DPDP Act 2023, Sec. 6 (Consent)	Capturing high-resolution images of individuals or private property without consent	High
 AI Object Rocession	IT Act 2000 Sec. 43A	Identifying persons/ vehicles without adequate security safeguards	High
 Real-time Processing	OST 1967 Art. VI	Using satellites for unauthorized military surveillance or weaponization	Medium
 Automated Decision-mking	DPDP Act 2023, Sec. 16	Denying benefits/services (e.g., disaster relief) based solely on automated AI outputs	High

Table 1. Technical and Legal Matrix

The first selected for the study is SkySat by Planet Labs, USA, which is a commercial optical microsatellite constellation (Planet Labs PBC, 2025). The second satellite selected for the study is RISAT-2B (ISRO, India), a state-operated X-band SAR platform (World Meteorological Organization, 2025). The third satellite is Gaofen-7 (CNSA, China), a state optical stereo mapping satellite (Tian et al., 2022). The fourth is the famous HawkEye 360 (USA), a private RF-signal geolocation constellation (HawkEye 360 Inc., 2025). The last one is Ofek-16 (Israel MoD), which is used in a military-grade electro-optical satellite Airforce (Technology.com, 2020).

If you closely observe, it is a unique combination of commercial and state-driven AI-powered satellites using varied modalities like optical, SAR, RF and geopolitically affecting India strategically.

6. ETHICAL STATEMENT

The project is desk-based, and human subjects were involved. Further, no classified data was accessed. It is based on international legal scholarship norms.

7. IN-DEPTH CRITICAL ANALYSIS OF DOMESTIC AND INTERNATIONAL LEGAL FRAMEWORK

One of the most important fundamental rights enshrined under Article 21 of the Constitution of India, 1950 (Nalwaya, Goswami, & Shastra, 2021), has been invoked to address the issue of privacy in the puttaswamy judgment (Supreme Court Observer, n.d.). If we observe closely, privacy can be intruded upon only with a specific justification, or there is an imminent need to protect the state's security and interests. The current privacy law completely neglects the continuous algorithmic tracking by commercial and government stakeholders.

The Digital Personal Data Protection Act defines data under section 2(t). "personal data" means any data about an individual who is identifiable by or about such data;" (Ministry of Electronics and Information Technology, 2024)

There is a lacuna in the law where there is a data breach only when directly attributed to the person. In the case of AI-satellite data breaches, the information collection may be based on the behaviour pattern of a crowd or location data. Data processing in India is covered under the act, but there is no provision to counter the extraterritorial data processing. The data will not be protected under the current law and is beyond the ambit of the law. Section 43A of the Information Technology Act, 2000, focuses primarily on IT system security breaches, but less on the security breaches by AI algorithmic processing and data processing by the AI-powered satellites.

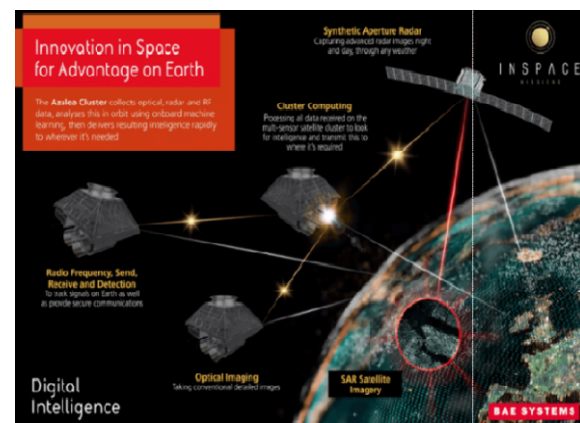
Article VI of the Outer Space Treaty, 1967 (United Nations Office for Outer Space Affairs, 1967; Kamenetskaya, E., 2015) requires the authorisation and continuous monitoring of space activities. The treaty was formulated before the upsurge of commercial satellites and Artificial intelligence. There are serious legal gaps in the treaty, wherein it fails to address the authorisation and supervision of commercial operators, and is silent on the flow of data and its governance. **UN Principles of Remote Sensing, 1986 Principle XII** (Sarin & Co. Legal, 2011) requires consultation before high-resolution images, but fails to

exercise its control effectively, and there is no enforcement mechanism.

8. SOVEREIGNTY AND SECURITY

Humans have, since the early ages, established territorial dominance. Power and domination have been key tools in acquiring natural resources and territories and dominance over human labour. At the international spectrum, this was reflected through the border divides and the establishment of sovereignty over the nations. The inordinate amount of development in the methods of warfare and investment made towards research and technology bespoke the covetous nature of those who wield power. Undoubtedly, the discovery of AI satellite surveillance led to its utilisation in politics, military, warfare, espionage and terrorism.

The militaries of various countries have been utilising the geo-spatial technology to access data on terrorist groups and internal threats, use satellite imagery to monitor movements, integrate GIS into remote sensing information and use GPS chips to detect locations (Kumar, 2022). Geo-spatial companies such as Maxar Technologies supply sensitive geo-spatial data, and the creation of a "virtual constellation of satellites" and the backend tech to integrate data from multiple sources allows for more frequent and comprehensive Earth observation, which improves decision making through rapid change detection, object recognition and predictive analytics, thereby playing a key role in national security (Zoldi, 2025). High-resolution satellite imagery, aerial captures from human-crewed and uncrewed aerial vehicles (UAVs/Drones), remote sensing, positioning systems is integrated with geo-spatial technologies to create what is known as Geo-spatial Intelligence which plays a critical role in the backbone of a country's military prowess and national security i.e. CAISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) (Singh, 2022).



Source: <https://innoter.com/en/articles/us-military-space-satellites/>

9. TECHNICAL ASPECT

Modern satellites have become advanced; they produce large quantities of raw data through raw imagery. Still, it was tough to process such vast amounts of data, but now the upsurge of AI has completely revolutionised it, making it very easy to analyse the raw data. Initially, the data was transmitted with limited

bandwidth and latency. In today's time, artificial intelligence is embedded in satellites or at ground stations where it is used to process the raw data. The AI-powered satellites can now analyse the images in real time, automatically identifying features such as ships, vehicles or infrastructure, detecting anomalies. The features are so advanced that the sensor can adjust to focus on emerging events. NASA's Dynamic targeting technology can track natural disasters in real time and reconfigure its system to improve observation with minimal human input (Defence.Capital, 2025).

These modern AI-powered satellites rely on several core technical elements like high-resolution optics or radar sensors, which enable the capture of detailed and high-resolution images across spectral bands. Furthermore, these satellites are equipped with advanced onboard computing, which allows them to process massive amounts of data. They also use machine learning algorithms to detect, classify and track the object and artificial intelligence to optimise satellite tasking. AI-powered satellites can convert discrete raw data into actionable intelligence in a fraction of the time.

Numerous real-world systems exemplify these advancements. Planet's SkySat constellation offers up to 0.5–0.9 m resolution with up to 10 daily revisits, using AI for object recognition, super-resolution imaging, and video analysis to support applications from agriculture to disaster response (European Space Agency, n.d.). India's RISAT-2B, a synthetic aperture radar (SAR) satellite, provides 0.3–1 m resolution in all weather, day or night, employing AI for change detection and surveillance analysis (Press Information Bureau, 2019). Japan's MHI AIRIS system integrates onboard AI to detect and track "dark ships" in real time for maritime security (Marine Insight News Network, 2024). Similarly, Starlink, while primarily a communications constellation, leverages deep learning for constellation control and secure traffic routing, offering civilian broadband and potential military communication capabilities (Outersputnik International Organization of Space Communications, 2025). Other systems, like JAXA's Deep Learning Attitude Sensor, enhance autonomous navigation and image-based decision-making in orbit.

These technologies come with dual use for military and civilian purposes. The satellite RISAT-2B is deployed for border safety through surveillance and intelligence gathering. The satellites of Starlink can immediately change their commercial activity into encrypted battlefield connectivity. Using satellites with such advanced abilities has led to economic development and national security planning. While simultaneously raising serious privacy and security concerns.

10. PRIVACY RISK

AI-enabled earth observation satellites have collapsed the distance between space and everyday life. It also indicates continuous scrutiny of human life. Resolution of constellations such as Planet SkySat now fuse sub-meter imagery with artificial intelligence to track crowd movement and structure creation. In 2022, during the Russian invasion of Ukraine, the SkySat satellite was able to trace the convoy of armoured military vehicles towards Kyiv. The satellite aid instant reporting compared to local reporters (Lyons & Richardson, 2023). SAR platforms like ISRO's RISAT-2B and China's

Gaofen-7 can give all-weather, day-night vision data. Amnesty International had relied on comparable SAR data to document the destruction of Rohingya villages in Myanmar despite monsoon cloud cover. Meanwhile, HawkEye 360 was able to track illicit fishing fleets—identifying hundreds of "dark ships" near the Galapagos in 2021, even when the vessels switched off their automatic identification beacons (HawkEye 360 Inc., 2020).

If we closely observe that India has enacted legislation for privacy protection, like the Digital Personal Data Protection Act, 2023 (Saha, 2024), The Information Technology Act 2000 (Ministry of Electronics and Information Technology, 2000) and the geo-spatial licensing rules. These laws specifically deal with terrestrial data flow. However, none of the laws focus explicitly on satellite imagery nor treat raw imagery metadata as personal data. So, satellites may take pictures of houses or car movements. You cannot claim any privacy as it is not legally protected. The rule focuses on who can sell or export the satellite data, but not on how often satellites can watch you, the reason behind their surveillance or where they store such data. This leaves a significant gap in people's privacy protection, wherein privacy can be easily violated through satellite data. One crucial development in the EU's General Data Protection Regulation (GDPR) (SecurePrivacy.ai, 2024) even if the satellite data is not directly related to a particular person, it can still protect the data, which indirectly highlights an individual's location, pattern or any sensitive images with the help of EU (GDPR). India should incorporate the same pattern in its law to make it more robust.

Today, because these AI-powered satellites are not regulated, they can continuously watch people, vehicles, or even daily activities from space without anyone knowing. Private organisations and governments can also keep track of entire cities, villages, and strategic locations like nuclear plants without any legal permission. As we have discussed, the data taken by these satellites has no legal protection under the law. It also violates one of the core principles enshrined under the Constitution of India, such as freedom and privacy. The collection of such data is also not in consonance with the Supreme Court's Puttaswamy doctrine (Supreme Court Observer (n.d.)). To address this crucial legal gap in our laws, the paper advocates expanding the statutory definitions of personal data to include satellite-derived imagery and metadata. Further, there should be a mandatory privacy impact assessment pre-launch for high-resolution missions. So that fundamental rights guaranteed by the Constitution of India do not become illusory rights.

11.ACCOUNTABILITYGAPS

The rapid proliferation of AI-powered commercial satellites has strengthened innovation but has significantly increased the regulatory and accountability risks at both the national and international levels. In the majority of jurisdictions, especially India, there is no comprehensive licensing governing the operation and data of AI-powered commercial satellites. State-owned satellites may undergo security and legal reviews. Startups and companies in space technology collect vital and sensitive data every day without any regulatory oversight in the guise of innovation. If we look at SkySat, which is managed by Planet Labs, and Hawkeye, which manages global imagery and tracks the geolocation of constellations registered in the USA,

the USA regulatory system (Doyon, 2022) focuses on control over exports and non-proliferation standards but hardly deals with privacy and data ethics. It enables these satellites to continue surveillance of the host nation with minimum policy control. In India, we have the Remote Sensing Data Policy and the National Geo-spatial Policy 2022 (Sarin & Co. Legal, 2011). This puts less emphasis on commercially operated and managed AI satellite surveillance.

In the absence of a comprehensive licensing policy, there is a lack of transparency. There can be instances where these private satellites must deliberately observe the urban infrastructure, sensitive sites, and population movement with minimal monitoring. The data from such satellites may be sold in international unregulated secondary markets. There is no watchdog or monitoring body to regulate and investigate the illegal activities of such commercial satellites and further enforce compliance with the legal norms against the commercial operators. If you observe closely, this leaves the individuals or communities legally unremedied for inappropriate surveillance. Most domestic laws, like DPDP Act 2023, do not have any mechanism to file complaints or provide compensation related to overhead satellite data, which is often processed internationally. Furthermore, regulatory responsibility is highly fragmented between ministries and agencies like ISRO, Department of Space, Ministry of Defence and regulators. Without a single body, serious risks related to privacy, security, or ethical controls are raised in real time (Pandey & Sharma, 2023). These gaps threaten individual rights and increase the risk of strategic, social, and humanitarian harm. The paper calls for an independent oversight body with powers to investigate and enforce, so that a balance can be struck between the human rights in the form of AI-powered satellites and core legal principles.

12. POLICY RECOMMENDATIONS AND A WAY FORWARD

12.1. AI GEO-SPATIAL SURVEILLANCE ACT

There is an imminent need for specific legislation to codify rights, duties, and redressal for vulnerable groups. This act should lay down a licensing and accreditation mechanism for state and private satellites by incorporating privacy impact assessment and AI-biased audits and ensuring compliance with technical legal matrices. There should be criminal, civil, and administrative recourse for misuse of AI algorithms and data breaches. It should also incorporate a mandatory human rights audit and echo the risk-based AI regulation system by drawing inspiration from the EU AI Act. The operators must secure renewable five-year licenses tied to legal compliance. There should be an introduction of extraterritorial provisions that would compel the foreign imagery vendors or brokers to appoint an Indian representative and submit to oversight following GDPR's representation rules. The penalties can be imposed based on turnover, and repeated violation can lead to cancelling the license or denying orbit use. This act will act as a catalyst for safeguarding privacy, security, and sovereignty.

12.2. INDEPENDENT OVERSIGHT AUTHORITY

The government should form an independent geo-spatial oversight authority (IGOA) to address accountability issues.

This body should be vested with quasi-judicial powers. The role of IGOA will enable the licensing of all the earth observation missions relating to India by private or public instruments. The authority should also register onboard AI assessment devices. The body should be empowered to regulate the launch of satellites only after proper privacy, legal and security checks. The body's investigation wing must comprise expert individuals who should be authorised to enter and inspect the ground stations, platform repositories, and downstream data brokers, and mandate data minimisation. Also, it should have the power to pass corrective orders or to impose pecuniary penalties. A board comprising technical experts, legal experts, and members of civil society with

special subject knowledge can publish a transparency report in coordination with sectoral regulators. The report will be presented before parliament for further appropriate action.

12.3. HUMAN RIGHTS IMPACT AUDIT

The effect of potential risks and threats calls for creating a human rights impact audit. On the international spectrum, human rights actors need to monitor and audit the impact of this technology. Moreover, shadow reports need to be made and submitted by the international NGOs to the international agencies, such as the United Nations and the Council of Europe, to protect human rights and ensure that they act as watchdogs to prevent the misuse of the technology and keep intact the sanctity of human lives.

12.4. DATA CATEGORISATION

The data collected through AI-powered geospatial satellites ought to be categorised into three distinct brackets: (i) Open Data, which can be freely accessed and disseminated without compromising individual rights or national interests; (ii) Critical Data, comprising datasets that directly impact governance, infrastructure, economic security, or essential public services, thereby requiring controlled access under licensing and monitoring mechanisms; and (iii) Sensitive Data, encompassing information relating to national security, defence installations, strategic locations, and personally identifiable or privacy-linked data, which must be subjected to the highest level of legal and technical safeguards.

The National Geospatial Policy, 2022, allows the processing of geospatial data in extraterritorial jurisdictions subject to supervision. This provision, when read in conjunction with India's obligations under the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the constitutional right of privacy recognised in Justice K.S. Puttaswamy v. Union of India (2017), raises serious concerns. Allowing sensitive datasets to be processed and stored outside India risks extraterritorial exposure, endangering India's data sovereignty, and fundamental rights of citizens.

It is therefore recommended that all Sensitive Data be mandatorily localised—stored and processed exclusively within India—under a robust statutory framework. Such localisation would not only align with constitutional mandates of sovereignty and privacy protection but also harmonise with international best practices such as the EU's General Data Protection Regulation (GDPR), which recognises location-linked and indirectly identifiable data as personal data. This

would ensure that privacy, sovereignty, and security remain legally safeguarded against both foreign state and non-state actors.

13. CONCLUSION

The study highlights a critical gap between technological innovations like AI-powered surveillance satellites and inconsistent legal norms. It establishes that the privacy laws cannot address the issue of extra-territorial and algorithmic surveillance. There is a lack of oversight and legal safeguards to address serious threats to our security and sovereignty. It also highlights that the laws relating to technology should keep pace with the development, or it would lead to serious consequences. Future research should explore ways technology can preserve the privacy, security, and sovereignty. The aim of policy-making should be to balance innovation and protecting rights, sovereignty, and security through proactive, collaborative governance. Without proper legal foresight, the AI-Powered satellite surveillance will affect the fundamental human rights, security, and sovereignty.

14. REFERENCES

- Amirfar, C., Popova, I. C., Tham, C. Y., & Marton, N. A. (2023, May 5). *Remote sensing from space: What norms govern?* Just Security. <https://www.justsecurity.org/86114/remote-sensing-from-space-what-norms-govern/>
- Chipatiso, E. (2024). Application of GIS and artificial intelligence in military operations: Prospects and challenges. *Space Science Journal*, 1(2), 1–7. <https://doi.org/10.33140/SSJ.01.02.06>
- Clarke, R. (1988). Information technology and dataveillance.
- Defence.capital. (2025, July 27). NASA's AI-driven dynamic targeting transforms satellite technology. *Defence.Capital*. <https://defence.capital/2025/07/27/nasas-ai-satellite-breakthrough-ushers-in-a-new-era-of-autonomous-earth-observation/>
- Doyon, M. (2022). The unregulated frontier: Privacy and ethics in commercial satellite imaging. *Journal of Space Law*, 47(1), 95–118.
- European Network of National Human Rights Institutions (ENNHRI). (n.d.). *Key human rights challenges of AI*. <https://ennhri.org/ai-resource/key-human-rights-challenges/>
- European Space Agency. (n.d.). *SkySat* [ESA Earth Online]. <https://earth.esa.int/eogateway/missions/skysat>
- Goldsmith, J., & Wu, T. (2006). *Who controls the Internet?: Illusions of a borderless world*. Oxford University Press.
- HawkEye 360 Inc. (2020, September 30). *Chinese fishing fleet encroaches on the Galápagos Islands*. <https://www.he360.com/resource/potential-illegal-fishing-seen-from-space/>
- HawkEye 360 Inc. (2025, June 25). HawkEye 360 to launch Cluster 12, expanding global signals intelligence constellation [Press release]. *PR Newswire*.
- Hobe, S., Schmidt-Tedd, B., & Schrogl, K. U. (Eds.). (2017). *Cologne commentary on space law* (Vol. 1). Carl HeymannsVerlag.
- Intersputnik International Organization of Space Communications. (2025, April 14). *Artificial intelligence and modern satellite communications*. <https://www.intersputnik.int/members-directory/?post=artificial-intelligence-and-modern-satellite-communications>
- Kumar, R. (2022). Significance of geo-spatial technology in national security: Indian perspective. *International Research Journal of Modernisation in Engineering Technology and Science*, 4(3), 621–624. <https://www.researchgate.net/publication/359203318>
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
- Lyall, F., & Larsen, P. B. (2018). *Space law: A treatise* (2nd ed.). Routledge.
- Lyons, D., & Richardson, A. (2023). The role of commercial satellites in the Ukraine conflict: A real-time AI imaging perspective. *Journal of Defence and Intelligence*, 15(1), 34–49.
- Marine Insight News Network. (2024, October 29). Mitsubishi unveils new AI-powered satellite system to track ship evasion. *Marine Insight*. <https://www.marineinsight.com/shipping-news/mitsubishi-unveils-new-ai-powered-satellite-system-to-track-ship-evasion/>
- Ministry of Electronics and Information Technology. (2000, October). *Information Technology (Certifying Authorities) Rules, 2000*. https://www.meitzy.gov.in/static/uploads/2024/03/IT-Act-Rules_2000_0.pdf
- Ministry of Electronics and Information Technology. (2024, June). *The Digital Personal Data Protection Act, 2023* (Act No. 22 of 2023).