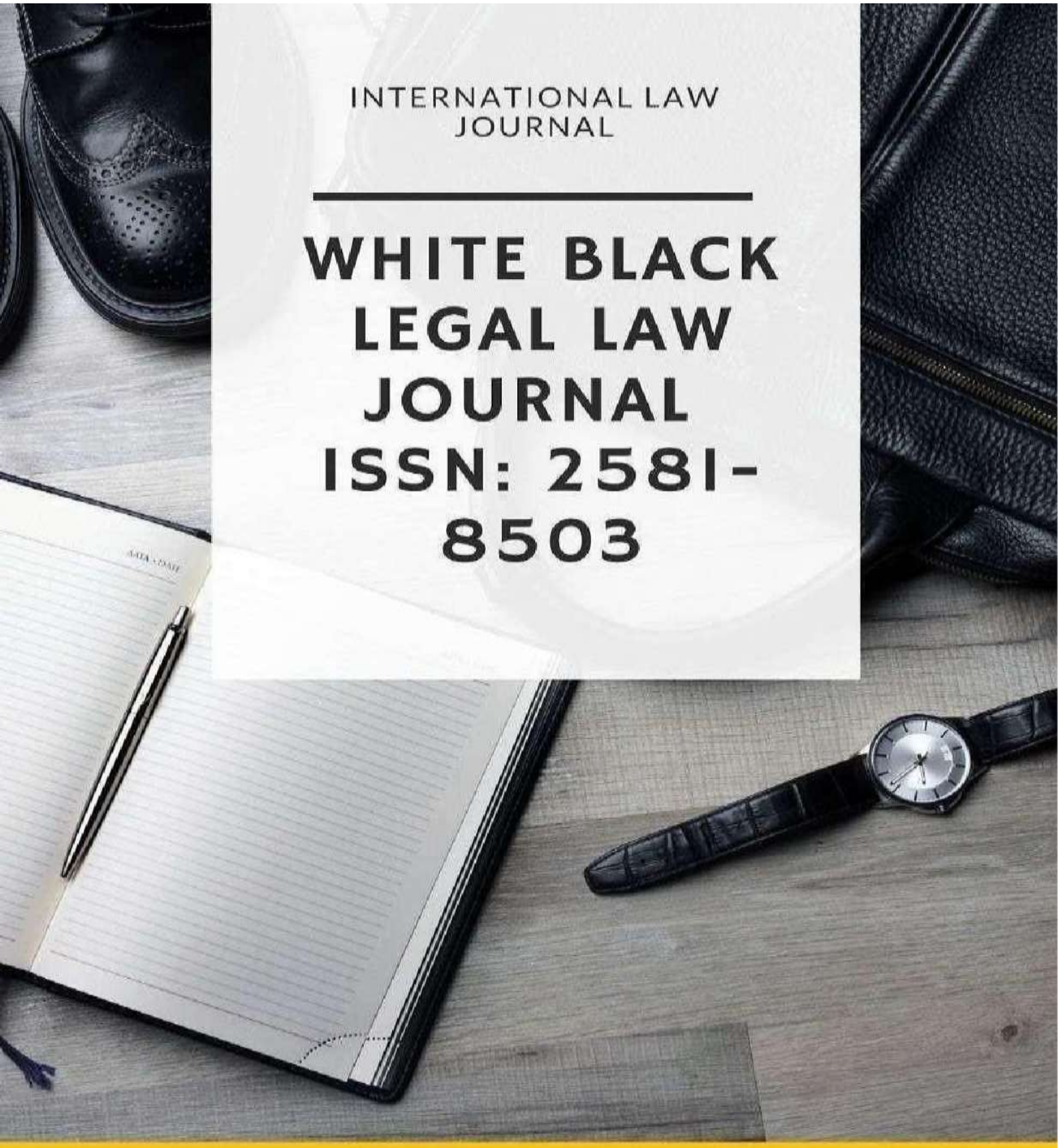

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

REMOTE SENSORS, GEOSPATIAL DATA AND IPR IN INDIA: LEGAL FRICTION IN A LIBERALISED ERA

AUTHORED BY - ADITHYA NARAYANAN

➢ Abstract:

The digital transformation of India largely relies on data collected via satellites, drones, and Internet of Things (IoT) sensors. Liberalisation of India's Geospatial Data Policy in 2021 permits foreign and private bodies to collect and freely exchange spatial data. Apart from enhancing innovation and monetary efficiency, it has raised new legal risks for safeguarding proprietary data, algorithms, and datasets. Remote sensors constantly record and reproduce information. This article identifies loopholes in India's IPR framework with respect to remote sensing, highlights the risk of data misappropriation, and compares international perspectives under TRIPS and the EU Database Directive. It ends with policy recommendations for accomplishing a balance between open geospatial access and intellectual property safeguard.
Keywords: *Geospatial data, remote sensing, database safeguard, intellectual property, international law.*

➢ Introduction:

Sensor-based data collection, along with remote sensing, has become a vital component of India's data-driven economy. From pollution assessment to management and precision farming, sensor systems generate a vast amount of geospatial data. Later Government of India realised its value through the *Guidelines for Acquiring and Producing Geospatial Data, and Geospatial Data Services* (Department of Science and Technology, 2021), liberalised the Remote Sensing Data Policy (RSDP 2011). The main aim of these reforms is to take away the licensing hurdles and open up for private participation.

Nevertheless, this policy shift has caused tension between data openness and intellectual property protection. It is easy through remote sensors to capture or reproduce protected materials such as maps, datasets, or imagery that constitute a significant intellectual investment. Therefore, this article determines how all these creations reveal flaws in present copyright, trade secret, and database protection mechanisms in India and contemplates reasonable reforms

as per global legal principles.

➢ Legal and Policy Background in India:

Earlier, India's remote sensing rules were prohibitive. Licenses to be obtained by the users from the National Remote Sensing Centre, as all high-resolution data are placed under government control by the RSDP 2011. After the advent of the Geospatial Data Guidelines of 2021, it has totally changed, deleting the majority of the licensing prerequisites, permitting Indian Companies to gather, retain, and distribute geospatial data freely, but confined to limited security restrictions. Thus, this refinement was to focus on enhancing investment and innovation in automated mapping and assessments.[1]

Still, India is not keeping up with respect to the intellectual property regime at the same speed as other sectors of development. Even though "original" artistic and literary works like maps are given copyright protection, it does not include facts or raw datasets. Only inventions are given patent protection, and do not include the collection of data. In case information becomes publicly available, then such confidential information is no longer confidential and thus not given protection. Unlike the Database Directive of the European Union, which protects collections formed with large-scale investment. Investing a huge amount of time and capital in building geospatial databases by companies may put their valuable data at risk of being copied, shared, or used without proper authorization or credit.[2]

➢ Why does this need quick legal solutions?

Remote sensors proliferated so rapidly that public risks and legal disputes are rising more quickly than legal protections. The following are the most urgent issues:

A. Intellectual property risks: copying, free-riding, and uncertain ownership-

A lot of companies invest a huge amount of time and try to collect and arrange geospatial data, like satellite pictures, drone maps, or location-based datasets. Yet, most sensor data is served as reliable information, and facts generally do not obtain strict copyright safeguards.

Because of this:

[1] *Resolving IPR Issues Relating to Geospatial Databases and GIS Products- A Pressing Priority for Geospatial Industry in India*, 30 J. INTELLECT. PROP. RIGHTS (2025), https://or.niscpr.res.in/index.php/JIPR/article/view/4305.
[2] *Id.*

- Other companies can gather similar data from open satellite or drone sources and develop nearly similar datasets.
- Portions of a diligently organised database may be taken and reused, without strict legal liabilities.
- Businesses may introduce products that might appear similar to the original dataset, but the law might not properly treat this as a violation.

Because there is no particular law that safeguards databases based on the hard work and investment used to develop them, not like in certain regions like the European Union.[3]

Also, recent regulations in India have made it simpler for several organisations to gather and publish geospatial data. As this helps develop innovation, it also raises the chances that valuable datasets may be misused or copied, making it difficult for original creators to safeguard their work.[4]

B. Privacy and Surveillance Risks:

Remote sensors gather plenty of information about people without direct interaction between them. For instance, they can record:

- Faces of Individuals via cameras,
- Where people move and travel,
- Vehicle number plates,
- Locations of people, and
- Regular behaviour, like when a person enters a place, and for what duration they stay there.

Generally, this data does not include a person's name. But even unnamed data may still recognise an individual. While distinct datasets are integrated, like location data, camera footage, and mobile data, it makes it easier to identify who the individual is. This method is termed re-identification.[5]

In India, the Digital Personal Data Protection Act, 2023, applies immediately once data directly or indirectly recognizes an individual. Which means organizations that gather or use sensor data should:

[3] *Id.*
[4] *Of Geospatial Data Deregulation, Intellectual Property and Personal Data Protection – SpicyIP*.
[5] *The Digital Personal Data Protection Bill, 2023*, (Aug. 3, 2023), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023?utm.

- Safeguard the data appropriately,
- Utilise it only for a specified purpose, and
- Notify authorities and affected individuals in case there is a data breach.

This is specifically significant as sensor data is frequently converted into analytics reports or dashboards and shared among other government bodies or private companies. If strict privacy protections are not adhered to, individuals' personal lives may be tracked without their knowledge or control.[6]

C. National security and sensitive mapping risks:

High-resolution mapping may disclose:

- Critical infrastructure layouts,
- Defence-sensitive regions,
- And sensitivities like power grids, telecom sites, pipelines.

India has historically led privileged disclosure via past remote sensing and mapping constraints, for instance, the RSDP framework for resolution screening. Security restrictions still exist in practice, even if liberalisation reduces licensing and remains a prime concern.

D. Drone and airborne sensor risks: safety + liability:

Drones are currently a significant form of remote sensing equipment. India's Drone Rules, 2021, lay down a framework for handling autonomous aircraft systems. This is significant as harm caused by the sensor is not only "data harm"; it can also cause physical harm (crashes, trespass, dangerous operations).

E. Cross-border data flows and global platform dominance:

At present, sensor data does not remain in one country. A usual pattern appears like this:

- Data is collected in India through satellites, drones, or sensors.
- Later, the data is moved to cloud servers located in another country.

[6] *Decoding India's DPDP Act: Your guide to protecting personal data*, (Feb. 3, 2026), https://www.acronis.com/en/blog/posts/decoding-indias-dpdp-act-your-guide-to-protecting-personal-data/?utm.

- Data is used by multinational enterprises for training AI models or developing analytics.
- The services or key takeaways are then resold to Indian users or the Indian government.[7]

This develops numerous issues:

Firstly, it creates confusion about who owns the data. Indian companies or agencies can collect the data, and foreign platforms may handle how it is stored, processed, and reused.

Secondly, it is tough to implement licenses. If the data was shared abiding by certain conditions, those rules are difficult to validate once the data moves out of India and is processed abroad.[8]

Thirdly, Indian legislation may not apply accurately. When servers, AI models, and companies are located outside India, authorities may encounter difficulties in monitoring unlawful use, investigating breaches, or applying penalties.

This risk is not notional. It is an element of how modern geospatial services and AI products are developed. In the absence of appropriate legal rules, Indian data may be misused commercially abroad with restricted safeguards for Indian users, creators, or regulators.[9]

F. "Model theft" and AI training on sensor data:

- **Prevailing international concern:** companies train AI models using remote-sensor data for crop prediction, mapping, and urban planning. If the training data is discarded or reused without authority:
  - Creators lose value, And the final product can function like a substitute for the real dataset.

[7] DATA FLOWS AND GOVERNANCE | OECD, https://www.oecd.org/en/topics/policy-issues/data-flows-and-governance.html (last visited Feb 3, 2026).
[8] Alexis Ditkowsky, THE ROLE OF CROSS-BORDER DATA FLOWS IN THE DIGITAL ECONOMY UNCDF POLICY ACCELERATOR (2025), https://policyaccelerator.uncdf.org/all/brief-cross-border-data-flows?utm (last visited Feb 2, 2026).
[9] Taxmann, CROSS-BORDER DATA TRANSFERS UNDER THE DPDP ACT 2023 TAXMANN BLOG (2025), https://www.taxmann.com/post/blog/cross-border-data-transfers-under-the-dpdp-act/?utm (last visited Feb 2, 2026).

- Old IP law grapples here, as "learning patterns" from data is not considered like copying a map.[10]

G. Accountability loopholes: who is liable when harm is caused?

Generally, remote sensor systems involve several different individuals and organisations, and not just one. For instance:

- One company may control the sensor (satellite, camera, drone),
- Another company may accumulate the data on a cloud server or platform,
- A different company may examine the data and develop reports,
- A government authority may make use of those reports to make decisions, and
- Other third parties may share or reuse the data later on.[11]

Since several actors are involved, it becomes hard to fix accountability at the time harm happens.

For example,

- If the privacy of people is infringed, it is not clear who failed to safeguard the data.
- If an incorrect map leads to financial loss, it is unclear who made the mistake.
- If an accident is caused by a drone, it is difficult to identify the operator, software company, or service provider is accountable.

As a consequence, implementation becomes ineffective. Victims might not know whom to complain against, and governance bodies may be reluctant to act, and companies might keep on blaming each other. This absence of clear accountability makes it difficult to restrict misuse and much more difficult to ensure justice at the time harm happens.[12]

➢ The Indian Legal and Policy landscape:

A. Geospatial Guidelines (2021): openness with limited prohibitions:

[10] RU-35-01-0053-280122/BACKGROUNDER THE DRONE RULES, 2021, https://static.pib.gov.in/writereaddata/specificdocs/documents/2022/jan/doc202212810701.pdf (last visited Feb 5, 2026).
[11] Jatinder Singh et al., *Accountability in the Internet of Things (IoT): Systems, Law & Ways Forward*.
[12] Young-Ju Kim, *Commercial Use of Satellite Remote Sensing Data and Civil Liability*, 13 LAWS 77 (2024), https://www.mdpi.com/2075-471X/13/6/77.

In 2021, the government of India implemented new geospatial guidelines to make it convenient for companies and startups to collect and utilise geospatial data. Previously, several authorizations were needed to create maps or gather location data. These guidelines rejected most of those approvals.

- What this means in practice:
    - Companies may now use drones, satellites, and sensors more freely.
    - Innovation and private investment have increased.
    - More maps, data products, and location services are being developed quickly.[13]
- The Issues:

  Since data collection is now simple, there is also a greater probability of:
    - Copying somebody else's data,
    - Unlawful use of sensitive information, and
    - Infringement of people's privacy.

  The policy focused more on innovation and growth, but it does not appropriately elaborate on how intellectual property and privacy issues must be controlled.[14]

B. The Remote Sensing Data Policy (2011):

- **How Remote Sensors threaten IPR:**

a) De facto copying and derivation risks-

Pictures of land and buildings, along with information, are collected continuously by Remote sensors. When arranging these data into maps or databases, it appears to be the same as the ones generally made by other companies. However, since only the design or creative part of a map is safeguarded by the Copyright law and excludes raw facts or coordinates, others can copy similar data and create the same products without technically violating the law. Which means creators of original works have limited control over their work being reused.[15]

[13] Na, INDIAN REMOTE SENSING DATA POLICY 2011 HIMALDOC (2025), https://lib.icimod.org/records/q0par-4b692?utm (last visited Feb 5, 2026).

[14] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited Feb 3, 2026).

[15] Of Geospatial Data Deregulation, Intellectual Property and Personal Data Protection – SpicyIP, *supra* note 4.

b) Loss of value for curated databases:

A huge amount of money and time is spent by companies while collecting, cleaning, and verifying geospatial data. Whereas remote sensors create the same data available freely, other players can rebuild those datasets easily at almost zero cost.[16] As India lacks such a special law that safeguards databases as the European Union does, these companies cannot prevent others from making use of their hard work. This discourages businesses from investing in better or more detailed data projects.[17]

c) Leakage of confidential information:

Data collected by sensors sometimes reveal details of private businesses, for instance, what crops are grown, where a factory is established, or what amount of material is produced. Where, because of data being shared publicly or combined with other open data, it can expose trade secrets of the company. In India, the law provides fewer safeguards for trade secrets, mostly through contracts, so once the data becomes public, companies can't safeguard much by themselves.[18]

d) Problems with licenses and enforcement:

Data quite often moves between different countries and cloud platforms, from sensors. It causes difficulty in tracing who owns what, at the time when people combine several data sources. Most of the users also neglect the license terms that prohibit how data can be used. Currently, India lacks a specialized system or authority to resolve disputes related to geospatial data licenses or to apply digital watermarking rules. This causes misuse and unlicensed use of valuable datasets to go unverified.[19]

C. Drone Rules, 2021- rules for sensor use via drones:

At present, the most common tools for remote sensing are drones. Basic rules are set by the Drone Rules, 2021, for:

- Registering drones,

[16] *Directive - 96/9 - EN - EUR-Lex*.
[17] *Unsd — Un-Ggim*, https://ggim.un.org/UN-IGIF/.
[18] WORLD INTELLECTUAL PROPERTY ORGANIZATION., WIPO GUIDE TO TRADE SECRETS AND INNOVATION. (2024), https://tind.wipo.int/record/49735.
[19] (Feb. 14, 2021), https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data_0.pdf.

- Acquire permission to fly,
- Identifying where drones can and cannot be used.

The loopholes:

Although these rules handle how drones fly, they do not properly explain:

- Who owns the data collected?
- Who is accountable for unlawful use of data, or
- How to manage privacy complaints.[20]

D. Digital Personal Data Protection Act, 2023- privacy rules for sensor data:

The DPDP Act, 2023, is India's major privacy law. It is applicable when data can identify an individual, even directly.

Why does this influence remote sensors:

- Sensor data may not contain names, but it may still show where an individual goes, what they do, or how they respond.
- When such data is examined, it becomes personal data as under the law.

What organizations are supposed to do:

- Utilize data only for a specified purpose
- Safeguard it from misuse or breach
- Remove it when it is no longer required, and
- Report severe data breaches.

The challenge:

Before the enactment of this law, several sensor systems were formulated. As a consequence, companies and government authorities are still uncertain about how to implement privacy rules for large-scale sensor data effectively.[21]

➢ International and Comparative Perspective:

- TRIPS Agreement, to which India is a signatory, sets minimum standards for protecting literary and artistic works, along with databases that have some originality. Since Countries are not forced to formulate special database laws. Therefore, it is up to each

[20] (Aug. 26, 2021), https://egazette.gov.in/WriteReadData/2021/229221.pdf.
[21] (Nov. 19, 2025), https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf.

country's choice with respect to how strongly it wants to preserve huge quantities of data collected.[22]

- The European Union has a dedicated law called the Database directive to safeguard even if they are not creative, as long as a huge amount of time, money, and effort went into creating them. This has enabled companies to build large databases, but few people are concerned that it may limit free access to public information.[23]
- The US does not have a dedicated database law. Whereas it safeguards data mostly through contracts and technology (like access control).
- India, yet, has started providing access to geospatial data, but does not have strong IP protections for people who spend on developing these datasets. This develops a problem, where Indian Companies' valuable data could be copied abroad in countries having better protection, but India itself does not offer similar safeguards.[24]
- Therefore, India seeks a balanced policy that maintains data to be open for innovation but also safeguards the hard work and investment of those who develop detailed datasets, along with adhering to TRIPS Rules.[25]

➢ Policy Responses and Recommendations:

- **Develop a law dedicated to safeguarding databases:**

  Few companies invest a huge amount of money and hard work to constitute a good geospatial database. A special law, like in the EU, ensures these efforts are safeguarded so others cannot copy their entire work freely. This safeguard must still allow the public to use basic data.[26]

- **Contracts and technology to be used to prevent misuse:**

  Companies must adopt tools such as digital watermarks or license tags on their data. These tools help to ensure that no other parties can copy the data without permission

[22] *Wto*, Overview of TRIPS Agreement https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm?utm.
[23] *Protection of Non-Original Databases*, https://www.wipo.int/en/web/copyright/activities/databases?utm.
[24] *SCCR/1/INF/3: Agenda Item 5: Protection of Databases. Information Received from Intergovernmental and Non-Governmental Organizations*, https://www.wipo.int/edocs/mdocs/copyright/en/sccr_1/sccr_1_inf_3.html?utm.
[25] *510700 Idea Jnl of Law & Tech.ps*, (Aug. 7, 2008), https://ipmall.law.unh.edu/sites/default/files/hosted_resources/IDEA/idea-vol45-no2-kumar-g.pdf?utm.
[26] Helga Tabuchi, *International Protection of Non-Original Databases; Studies on the Economic Impact of the Intellectual Property Protection of Non-Original Databases*, 3 DATA SCI. J. 175 (2004), http://datascience.codata.org/articles/abstract/10.2481/dsj.3.175/.

and make it easy to track who used it.[27]

- **Government body to be constituted to look over geospatial data:**
  An exclusive authority under the Department of Science and Technology must verify whether big data industries adhere to the rules, whether data is appropriately used, and whether sensitive information is safeguarded. Thus, innovation goes on, while ensuring that there is no such misuse.[28]
- **Obliging several government bodies to function together:**
  Agencies must collaboratively work while handling IP, space data, and national security.
- **Work along with the international organization:** India, to ensure its companies' funding in data receives appropriate acknowledgement and safeguards in world markets, and must communicate to the global bodies such as WIPO and WTO.[29]

➢ Conclusion:

India's initiative with respect to opening its geospatial sector data is a stepping stone towards a data-driven economy. However, in the absence of relevant intellectual property safeguards, the liberalised governance might cause risks, weakening data quality and private innovation. Remote sensors expand such risks by developing duplication without much effort. A fair approach, implanted in TRIPS principles, endorsed by technical and contractual protections, and directed towards barely modified database safeguard, which can assist India to balance both originality and openness in its geospatial environment.

[27] Dominique Guinard, *C2PA 2.1 - Strengthening Content Credentials with Digital Watermarks*, Strengthening Content Credentials with Digital Wat (Aug. 27, 2024), https://www.digimarc.com/blog/c2pa-21-strengthening-content-credentials-digital-watermarks.
[28] *National Geo-Spatial Service Portal*, https://geospatial.dst.gov.in/Guidelines.aspx?utm.
[29] *Line of Work - Integrated Geospatial Information Framework*, UN-GGIM Europe (Feb 25, 2026), https://un-ggim-europe.org/working-groups/line-of-work-integrated-geospatial-information-framework/.