

Original Research

Received 24 May 2026

Revised 27 June 2026

Accepted 19 July 2026

Natural Resources for Human Health 2026, Vol. 6 (9s): 782–798

KEYWORDS:

Earth Observation Satellites, Remote Sensing, Data Privacy, Digital Personal Data Protection Act, 2023 (DPDP Act)

Earth Observation Satellites and the Right to Privacy: Towards A Regulatory Framework for Satellite-Derived Personal Data in India

Akshay Garg¹, Dr. Ramakant Tripathi², Jahnnvi Mishra³, Harsh Vardhan Srivastava⁴

¹Research Scholar in Law (Ph.D. Pursuing), Law College Dehradun, Uttaranchal University, Prem Nagar- 248007, Dehradun, Uttarakhand, India.

akshaygrg756@gmail.com ORCID ID: 0009-0004-1819-1367

²Associate Professor, Law College Dehradun, Uttaranchal University, Prem Nagar- 248007, Dehradun, Uttarakhand, India.

ramakanttripathi91@gmail.com ORCID ID: 0009-0000-0302-7741

³School of Law, Shri Vile Parle Kelvani Mandal's Narsee Monjee Institute of Management Studies (Deemed to be University), Mumbai, India.

jahnnvi.521@gmail.com ORCID ID: 0009-0000-1752-2364

⁴School of Law, , Shri Vile Parle Kelvani Mandal's Narsee Monjee Institute of Management Studies (Deemed to be University), Mumbai, India.

srivastavaharsh1221@gmail.com ORCID ID: 0009-0006-2217-7626

ABSTRACT: The increase in the number of Earth Observation satellites has significantly transformed the technology of remote sensing from being a state monopolised tool to commercially available technology, capable of real time surveillance of individual, property and territory. The principles by United Nation in respect to the remote sensing of the earth from outer space 1986 has been the fundamental principle for the governance of EO activities. These principles were formulated decades before the emergence of artificial intelligence, big-data analytics, and commercial satellite imagery markets. Consequently, these guidelines remain ineffective on matters of data privacy or the classification of satellite-derived information as personal data. The present article examines the India's Digital Personal Data Protection Act, 2023, along with other space policies which is capable of addressing the present issue of privacy and surveillance.

Using a doctrinal and comparative methodology, the present article showcases that neither the international law nor the national law of India addresses the issue of privacy arising from Earth Observation satellites. The legal framework fails to differentiate between the personal data and non-personal geospatial data. Additionally, it lacks in imposing obligations related to specific satellite base data collection and therefore leaving a significant gap in accountability and individual redress.

1. INTRODUCTION

1.1 Background and Context

Outer space activity has undergone a fundamental transition from being a sector monopolised by state to cold war era enterprise and finally into a diversified commercial industry in the present time which is driven by private capitals and rapid technological innovation. [1] This shift can be understood with the pronounced field of Earth Observation (EO), initiated by the government operated satellites such as Landsat and SPOT that was launched primarily for scientific and metrological purposes but now has evolved into a commercial ecosystem that is operated by operators such as Planet Labs, Maxar Technologies and ICEYE, these

operators are capable of imaging virtually any point on the Earth's surface at sub-metre resolution, often on a daily basis. [2] This capability has generated substantial value across agriculture, disaster management, urban planning and national security. [3] At the same time, the capacity that allows a satellite to track deforestation or flood damage also allows it to observe individual vehicles, dwellings and patterns of human movement, creating an unprecedented surveillance capability that existing legal frameworks, international and domestic, were never designed to address. [4]

1.2 Research Problem

International space law, principally the Outer Space Treaty, 1967 and the United Nations Principles Relating to Remote Sensing of the Earth from Outer Space, 1986, was negotiated at a time when remote sensing was the exclusive preserve of a handful of States and lacked the resolution, frequency and analytical capability of contemporary commercial satellites. These instruments accordingly draw no distinction between personal and non-personal satellite-derived data, and are silent on issues of individual privacy. At the domestic level, India's Digital Personal Data Protection Act, 2023 (DPDP Act) was designed principally around the digital, consent-based collection of personal data by data fiduciaries, and does not squarely address passive, non-consensual collection of geospatial information by satellites orbiting hundreds of kilometres above the data subject. The result is a regulatory vacuum: satellite-derived personal data in India is governed neither comprehensively by international remote sensing law nor meaningfully by the domestic data protection regime.

1.3 Scope and Limitations

The study is confined to the legal and regulatory dimensions of EO-derived privacy concerns and does not examine the technical or engineering aspects of satellite sensor design except where directly relevant to the legal analysis. The international law analysis is limited to the instruments most directly relevant to remote sensing and privacy, namely the Outer Space Treaty and the 1986 Remote Sensing Principles, rather than the full corpus of UN space treaties. The domestic analysis focuses on India. Military and intelligence applications of EO technology are noted only insofar as they inform the broader regulatory discussion, since classified national security uses fall outside the scope of a civil law-oriented inquiry.

2. EVOLUTION OF EARTH OBSERVATION TECHNOLOGY AND EMERGING PRIVACY CONCERNS

2.1 Understanding Earth Observation Satellites

Earth Observation satellites are spacecrafts that are equipped with sensors especially designed to capture information about the Earth's surface, atmosphere and oceans. [5] They are generally classified according to the type of sensor that is employed such as optical satellites capture imagery within the visible and near-infrared spectrum, while Synthetic Aperture Radar (SAR) satellites use active radar signals that is capable of penetrating cloud cover and operating irrespective of daylight conditions. [6] The proliferation of small satellite constellations, comprising dozens or even hundreds of individual spacecraft, has dramatically increased revisit frequency, with some commercial operators now capable of imaging a given location multiple times within a single day. [7]

2.2 Evolution from Government-Controlled Remote Sensing to Commercial EO Markets

Remote sensing as a concept came as an exclusively governmental activity that was exemplified by the United States Landsat Programme, initiated in 1972, and the French SPOT programme, which prioritised scientific and meteorological objectives over commercial exploitation. [8] Liberalisation began in the United States with the Land Remote Sensing Commercialization Act, 1984 and its successor, the Land Remote Sensing Policy Act, 1992, which permitted licensed private operators to sell satellite imagery commercially, subject to oversight by the National Oceanic and Atmospheric Administration. [9] This liberalisation, paralleled by the Commercial Space Launch Competitiveness Act, 2015, enabled the emergence of dedicated commercial EO operators. [10] The European Union pursued a parallel trajectory through Copernicus, which, while retaining a governmental character, adopted a full, free and open data policy, distinguishing it from the licensed-commercial American model. [11] The resulting global market now comprises government-operated systems, open-data programmes, and purely private constellations offering sub-metre resolution imagery on a subscription basis. [12]

2.3 Artificial Intelligence, Big Data and Satellite Data Analytics

The privacy implications of the contemporary EO technology cannot be assessed unless we draw a reference to raw imagery alone. Modern satellite operators are increasingly deploying artificial intelligence and machine-learning tools that process out

volumes of imagery into structured and analysed datasets. There are automated object detection algorithms which can identify, count vehicles, track ship movements, monitor construction activity, or detect changes in land use over time. [13] When integrated with big data analytics platforms, these tools can be very useful as they generate temporal patterns of activity at a specific location, effectively producing behavioural profiles without requiring any human interpretation of the underlying imagery. [14] Because the 1986 Remote Sensing Principles were drafted more than a decade before the commercial availability of high-resolution imagery and several decades before the emergence of AI-enabled analytics, they provide no guidance whatsoever on the privacy implications of automated, large-scale interpretation of satellite data. [15]

2.4 When Does Geospatial Information Become Personal Data?

The point at which geospatial information crosses the threshold into "personal data" is not self-evident and depends upon several interacting factors. The first is resolution: imagery capable of resolving individual vehicles, building entrances or, increasingly, individual persons raises materially different privacy concerns from imagery depicting broad land-use patterns. [16] The second is combinability: even moderate-resolution imagery, when combined with cadastral records, mobile location data or social media geotags, can enable re-identification of specific individuals or households, a risk well documented in the broader data protection literature on anonymisation and re-identification. [17] The third is persistence and frequency: a single image of a location carries limited privacy risk, whereas a temporal series of images revealing arrival and departure patterns at a specific address begins to resemble continuous surveillance. [18] On this basis, satellite-derived geospatial data should be treated as personal data whenever it is capable, whether alone or in combination with other reasonably available information, of identifying a specific natural person or of revealing information about an identifiable individual's location, movements, or activities at a specific address.

2.5 Privacy Risks Associated with Contemporary EO Technologies

The convergence of high-resolution imaging, high revisit frequency and AI-enabled analytics generates several distinct categories of privacy risk. First, there is a risk of covert surveillance of individuals or households, since satellite monitoring, unlike terrestrial CCTV, requires no physical access to the target location and leaves the data subject with no meaningful opportunity to detect or object to the collection. [19] Second, there is a risk of commercial profiling, where inferred data concerning property use, vehicle ownership or agricultural activity is commercialised without the knowledge or consent of affected individuals. [20] Third, there is a risk to national security, since high-resolution imagery of sensitive installations may be exploited by hostile actors notwithstanding its lawful commercial availability. [21] Finally, there is a broader chilling effect, whereby the mere possibility of persistent satellite observation may discourage lawful activity, a concern increasingly recognised in privacy scholarship on aerial and satellite surveillance. [22]

3. INTERNATIONAL REGULATION OF EARTH OBSERVATION: A LEGAL FRAMEWORK IN TRANSITION

3.1 Development of International Remote Sensing Law

The legal regulation of remote sensing activities developed gradually within the Committee on the Peaceful Uses of Outer Space (COPUOS), beginning in the early 1970s as the Landsat programme demonstrated the practical capability of satellites to observe the territory of other States without their consent. [23] Developing States, in particular, expressed concern that unrestricted remote sensing of their territory by technologically advanced States could compromise their sovereignty and economic interests, since sensing States would obtain valuable resource and agricultural data concerning foreign territory before the sensed State itself. [24] These concerns produced more than a decade of negotiation within COPUOS, ultimately culminating in the adoption of the Principles Relating to Remote Sensing of the Earth from Outer Space in 1986. [25] As with much of the international space law framework, this instrument took the form of a non-binding UN General Assembly resolution rather than a treaty, reflecting the difficulty of securing binding consensus on an issue implicating both sovereignty and the free-use principles of the Outer Space Treaty. [26]

3.2 The Outer Space Treaty and the Principle of Freedom of Exploration

The legal legitimacy of remote sensing activity rests upon Article I of the Outer Space Treaty, 1967, which establishes that the exploration and use of outer space shall be carried out for the benefit of all countries and shall be free for exploration and use by all States without discrimination, including freedom of scientific investigation. [27] This principle has consistently been

interpreted to permit States and, by extension, their licensed private operators, to conduct remote sensing of any part of the Earth's surface, including the territory of other States, without requiring the prior consent of the sensed State. [28] Article II's principle of non-appropriation reinforces this position by confirming that no State may assert sovereignty over outer space itself, though it has no direct bearing on activities conducted on the Earth's surface that are merely observed from orbit. [29] The consequence of this framework is that the "freedom to sense" is treated as an extension of the general freedom of use of outer space, with no corresponding textual obligation in the Outer Space Treaty to protect the privacy of individuals located within the sensed territory. [30]

3.3 State Sovereignty, Open Access and Data Sharing

The tension between sovereignty and open access identified during the drafting of the 1986 Principles persists in contemporary practice, though it has evolved considerably. The European Union's Copernicus programme exemplifies a full, free and open data policy, under which processed satellite imagery is made available to any user without charge, on the premise that broad accessibility maximises the societal and scientific value of EO data. [31] This approach stands in contrast to the licensed-commercial model adopted in the United States, where high-resolution imagery is typically sold under commercial terms subject to federal licensing conditions administered by the National Oceanic and Atmospheric Administration. [32] Both models, however, share a common feature relevant to the present inquiry: neither the open-access nor the commercial-licensing approach incorporates any mechanism requiring the sensing operator to assess whether the data being shared or sold reveals identifiable information about specific individuals, since both frameworks were designed to regulate the flow of data between States and commercial entities rather than to protect individual data subjects. [33]

3.4 Limitations of the Present International Framework

The international remote sensing law framework suffers from several interlocking limitations when assessed against contemporary privacy challenges. First, it lacks any binding instrument, since the 1986 Principles remain a non-binding General Assembly resolution, leaving States free to disregard even its state-centric provisions. Second, it contains no classification distinguishing personal from non-personal satellite-derived data, an omission that becomes increasingly significant as processed and inferred data approach the specificity of individually identifiable information. Third, it establishes no institutional mechanism, whether within COPUOS or otherwise, capable of receiving complaints or developing guidance responsive to AI-enabled analytics. Fourth, it does not address the accountability of private commercial operators, having been drafted when remote sensing was conducted almost exclusively by States. These limitations confirm that the privacy dimension of satellite-derived data must, for the foreseeable future, be addressed principally through domestic legal frameworks, examined next with reference to India.

4. INDIA'S LEGAL FRAMEWORK GOVERNING SATELLITE DATA AND PRIVACY

4.1 India's Expanding Earth Observation Ecosystem

India has developed and become an extensive government operated Earth Observation programmes among the rest of the spacefaring nations. There are missions like Cartosat, RISAT and EOS series which were operated by Indian Space Research Organisation (ISRO), these missions collectively provided high-resolution optical and radar imagery which was used for the for agricultural monitoring, disaster management, urban planning and national security purposes. [34] This capability of government has been increasingly complemented by the private companies as in August 2025, IN-SPACE had selected a consortium by Pixxel and with Dhruva Space, PierSight and SatSure. Together under a Public-Private Partnership, these firms build India's first fully indigenous private EO satellite constellation which integrated optical, hyperspectral and Synthetic Aperture Radar payloads. [35] This growth in both governmental and private EO capability has significantly increased the volume and resolution of satellite-derived data concerning Indian territory and its residents, without a corresponding expansion of the legal framework governing the privacy implications of that data. [36]

4.2 IN-SPACE and the Commercialisation of Remote Sensing

The Indian National Space Promotion and Authorisation Centre (IN-SPACE) was originally established as the single-window authorisation and a promotional body that can work for non-governmental space activities which also includes remote sensing and EO services. [37] Its establishment is a significant institutional reform, providing private EO operators with a defined authorisation pathway that did not previously exist in comprehensive form. [38] However, this mechanism operates in the

continued absence of comprehensive parliamentary legislation governing India's space sector, meaning that licensing standards, supervisory procedures and enforcement powers rest primarily on executive guidelines rather than statutory provisions. [39] This creates particular uncertainty for satellite-derived personal data, since IN-SPACE's authorisation framework is oriented principally towards technical, safety and strategic considerations, rather than the data protection obligations of the operators it authorises. Consequently, an EO operator may satisfy every applicable IN-SPACE requirement while remaining entirely unconstrained by any privacy-specific obligation concerning the imagery or analytics it subsequently commercialises. [40]

4.3 National Geospatial Policy and Satellite Data Governance

India's approach to the governance of geospatial data more broadly was substantially liberalised through the Guidelines for Acquiring and Producing Geospatial Data, 2021, and subsequently the National Geospatial Policy, 2022, both of which removed longstanding restrictions on the acquisition, ownership and commercial use of geospatial data, including satellite imagery, by Indian private entities. [41] This liberalisation replaced a prior regime of prior governmental scrutiny with a self-certification model, under which private entities are permitted to collect and deal in geospatial data, including high-resolution satellite imagery, without seeking prior approval, subject only to specified negative lists restricting particularly sensitive strategic locations. [42] While this reform has been instrumental in enabling the growth of India's private EO sector discussed above, neither the 2021 Guidelines nor the 2022 Policy contain any provision addressing the privacy of individuals whose property, movements or activities may be captured within geospatial datasets, since both instruments were framed principally to advance economic liberalisation and self-reliance objectives rather than data protection objectives. [43] The result is a governance framework that actively facilitates the commercial generation and circulation of high-resolution geospatial data concerning Indian territory, without any accompanying safeguard addressing the personal data risks identified in Section II. [44]

4.4 Applicability of the Digital Personal Data Protection Act, 2023 to EO Data

The Digital Personal Data Protection Act, 2023 governs the processing of “personal data” within India, defined under Section 2(t) as any data about an individual who is identifiable by or in relation to such data, where that data is processed in digital form. [45] This definition is broad enough to capture satellite-derived data that identifies a specific individual, such as imagery or analytics revealing activity at a particular residence. [46] However, the Act's operative architecture is built around a consent-and-notice framework under Sections 5 and 6, which contemplates a data fiduciary collecting personal data from, or with the knowledge of, a data principal, together with “certain legitimate uses” exemptions under Section 7 that similarly presuppose some interaction between fiduciary and principal. [47] Satellite-derived collection, by contrast, is entirely passive: an individual whose property or movements are captured from orbit has no opportunity to receive notice, grant or withhold consent, or otherwise interact with the data fiduciary at the point of collection. The Act contains no provision, analogous to those in some comparative frameworks for publicly observable or ambient data, addressing this category of passive, remote collection, leaving uncertainty as to whether EO operators are expected to comply with its consent architecture at all. [48]

4.5 Personal Data versus Geospatial Data under the DPDP Framework

This uncertainty is compounded by the absence of any statutory guidance on when geospatial data crosses the threshold into “personal data” under the DPDP Act. Applying the identifiability test developed in Section 2.5 to the definition under Section 2(t), raw satellite imagery of a wide geographic area would ordinarily fall outside personal data, since no specific individual is identifiable from the imagery alone. [49] However, processed or derived data narrowed to a specific address, particularly when combined with land-ownership records, mobile location data or other reasonably available datasets, would appear to satisfy the statutory identifiability threshold. [50] The Act offers no interpretive guidance, whether through the statute or subordinate rules, on how this combinability-based test should be applied to geospatial datasets, nor whether aggregated or anonymised analytics, such as area-wide vehicle counts, ought to be treated differently from address-specific analytics. [51] This gap is significant given that the Act's anonymisation exemptions presuppose a reliable standard of irreversible de-identification, difficult to satisfy in the geospatial context precisely because of the re-identification risk created by combining imagery with other available datasets. [52]

4.6 Constitutional Privacy Jurisprudence and Satellite Surveillance

The absence of a specific statutory response to the surveillance of satellites has to be assessed against the constitutional privacy jurisprudence of India, that has developed independently and also in absence of DPDP Act. In case of *Justice K.S. Puttaswamy (Retd.) v. Union of India* [(2017) 10 SCC 1], a nine-judge bench of Supreme Court ruled out unanimously that right to privacy is a

fundamental right and therefore it is protected under Article 21, read with Article 14 and Article 19 of the Constitution. [53] The majority in this case also brought up a threefold test of legality, legitimate aim and proportionality which has to be satisfied by the actions of the State. [54] This framework was elaborated further in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (the Aadhaar judgment) [(2019) 1 SCC 1], where the majority held out a more granular four-part test of proportionality which required a legitimate aim, a suitable means of achieving it, the absence of any less restrictive but equally effective alternative, and an assessment of whether the measure disproportionately burdens the right holder. [55] This proportionality framework, reinforced by earlier surveillance jurisprudence such as *People's Union for Civil Liberties v. Union of India* [(1997) 1 SCC 301] concerning telephone interception, provides a constitutional benchmark against which any governmental use of satellite surveillance capability ought to be assessed. [56] At present, neither the IN-SPACe authorisation framework nor the National Geospatial Policy, 2022 incorporates any proportionality-based safeguard of this kind, meaning satellite-derived surveillance capability currently operates without the procedural and substantive constraints this jurisprudence would appear to require. [57] This constitutional gap reinforces the case, developed throughout this paper, for a dedicated regulatory framework addressing satellite-derived personal data in India.

5. REGULATORY GAPS IN GOVERNING SATELLITE-DERIVED PERSONAL DATA

5.1 Absence of Legal Classification of Satellite-Derived Personal Data

The Digital Personal Data Protection Act, 2023, defines personal data as any data through which an individual is identifiable by or in relation to such data. [58] This definition was drafted keeping in mind the conventional data flows which includes the names, financial records, biometric identifiers, communication metadata, sort of information that comes from a person's direct interaction with a digital service. [59] Satellite-derived geospatial data is not covered under this definition, and the law makes no attempt to incorporate it. [60] Neither, in the Act, nor in the rules framed under it, does the legislature address the question of privacy infringed by the data layer captured from orbit. [61]

This is not a significant omission. A satellite image of a residential plot may reveal nothing more than a rooftop. However, the same images, when run through a pattern-of-life analysis or cross-referenced with cadastral records, vehicle movement, or thermal signatures, can reveal various occupancy patterns, it can reveal the presence of specific individuals, or even health-related inferences, for instance irregular movement may suggest illness or disability. [62] The DPDP Act provides no threshold, no test, and no interpretive guidance for determining at what point raw geospatial output becomes identifiable personal data through enrichment or fusion with other datasets. [63] It was simply not built to that gap, because Earth Observation was not part of the legislative imagination when the law was conceived.

India's space governance tools are no better. The Norms for Private Sector Participation in Space Activities, along with the IN-SPACe authorisation framework, regulate resolution thresholds and licensing conditions for commercial satellite operators, but these instruments are concerned with only the national security clearance and export control, not with the informational privacy of individuals who happen to fall within a satellite's field of view. [64] There is, at present, no law in India for satellite-derived personal data as a distinct class of information requiring its own consent architecture, retention limits, or purpose-specification requirements. [65]

The consequence of this vacuum is that Earth Observation operators in India currently function in a space where their output is treated, automatically as default, as raw commercial or scientific data instead than the data capable of infringing an individual's privacy. This sits contrary with the reasoning in *Justice K.S. Puttaswamy v. Union of India*, where the Supreme Court recognised “informational privacy as an inseparable facet of the right to life and personal liberty under Article 21”, which extends the protection to information that can be covered together to make a profile of a person's life. [66] A legal tool that fails to even name a satellite-derived personal data as a category cannot meaningfully operationalize that constitutional guarantee in the EO context, and this gap in the classification is the foundation from which the remaining regulatory deficiencies examined in this Part follows.

5.2 Consent and Notice in Passive Satellite Data Collection

The DPDP Act builds its entire architecture around the consent of the data principal, obtained through a notice that specifies the purpose of collection. [67] This model presumes a point of interaction, a form filled, an application installed, a checkbox ticked, at which the individual can exercise a meaningful choice. [68] Satellite observation collapses this premise entirely. A person standing in their courtyard, driving along a highway, or attending an outdoor gathering has no opportunity to consent

to being imaged, because they are usually unaware that a satellite is passing overhead with a sensor capable of resolving objects to sub-metre accuracy. [69]

This is what might be termed passive collection, gathering of data without any transaction, request, or notice directed at the individual concerned. The consent-notice model, whatever its merits for platform-based data collection, is structurally incapable of application here. Even the exemptions carved out under Section 7 of the DPDP Act, for purposes such as employment or compliance with law, do not contemplate a scenario where an entire population within a satellite's swath width becomes a data subject by virtue of geography alone. [70] Nor does the Act's provision for deemed consent offer real assistance, since deemed consent still requires some contextual relationship between the data principal and the fiduciary, a relationship that plainly does not exist between an individual on the ground and a commercial EO operator orbiting several hundred kilometres above. [71]

Comparable difficulties have been noted in the aerial surveillance and drone context internationally, where regulators have generally responded not by insisting on individual consent, which is impossible to secure, but by regulating the purpose, resolution, and retention of imagery instead. [72] India's regulatory framework has not yet made this conceptual shift for satellite imagery. The result is a legal fiction in which every EO operation involving inhabited terrain is, strictly read, non-compliant with the consent requirements of the DPDP Act, a fiction that persists only because no one has yet tested it before a court or the Data Protection Board.

5.3 Accountability of Commercial Earth Observation Operators

The DPDP Act imposes obligations on data fiduciaries, entities that determine the purpose and means of processing personal data. [73] Commercial EO companies operating under IN-SPACe authorisation sell imagery and derived analytics to government departments, insurers, agricultural technology firms, and increasingly to private clients engaged in competitive intelligence or property surveillance. [74] Yet whether such a company qualifies as a data fiduciary at all remains unresolved, because that classification depends on the imagery first being recognised as personal data, which, as discussed above, is not settled.

Even assuming fiduciary status were established, the accountability structure built into the DPDP Act does not map neatly onto the EO value chain. Raw imagery is typically captured by the satellite operator, processed and enriched by a separate analytics firm, and then licensed onward to an end user who applies it for a specific commercial purpose. [75] Each of these actors handles the data differently, and the Act's fiduciary-processor distinction was designed for far simpler outsourcing arrangements, such as a company using a third-party cloud vendor, not for a multi-tiered chain in which the entity that captures the data is rarely the entity that ultimately profiles the individual. [76]

IN-SPACe's authorisation process focuses on licensing the satellite operator for launch and operation, verifying resolution limits against national security guidelines, and ensuring compliance with foreign exchange and export control norms. [77] It does not require operators to demonstrate a data protection impact assessment, appoint a data protection officer, or maintain records of onward disclosure of imagery involving identifiable individuals or their property. [78] Consequently, an EO operator can remain in full compliance with its space-sector licence while having no accountability whatsoever under data protection law for how its imagery is subsequently used to build behavioural or locational profiles of specific persons.

5.4 Data Processing, Storage and Cross-Border Transfers

Satellite imagery, once captured, rarely stays within a single jurisdiction. Ground stations may be located in one country, processing infrastructure in another, and the end client in a third. [79] India's DPDP Act permits cross-border transfer of personal data except to countries specifically restricted by the Central Government, a negative-list approach that is comparatively permissive when set against the adequacy-based model of the European Union. [80] For most categories of personal data this permissiveness may be defensible, but satellite-derived data raises distinct concerns because of its capacity to reveal sensitive locational information about critical infrastructure, defence installations, and vulnerable populations, alongside ordinary residential areas. [81]

The Act does not currently carve out any sector-specific restriction for geospatial data transfers, despite the fact that India's own space policy treats resolution and distribution of high-resolution imagery as a matter requiring case-by-case governmental clearance for reasons of national security. [82] There is an unresolved tension here: the space regulatory regime treats high-resolution EO data as sensitive enough to require pre-clearance for distribution, while the data protection regime, once that

imagery is licensed onward, imposes no equivalent scrutiny on where it is stored, how long it is retained, or which foreign entities may access it for analytics purposes. Storage limitation, one of the core data protection principles embedded in Section 8 of the DPDP Act, is difficult to enforce in practice for satellite archives, which are commercially valuable precisely because of their historical depth, and where operators have strong incentives to retain imagery indefinitely for time-series analysis rather than delete it once the original purpose has been served. [83]

5.5 Transparency, Individual Rights and Remedies

The rights conferred on a data principal under the DPDP Act, the right to access information about processing, to correction and erasure, and to grievance redressal, presuppose that the individual knows a data fiduciary is processing their data in the first place. [84] In the EO context this knowledge almost never arises. A landowner whose property has been repeatedly imaged and analysed for change detection, an individual whose movements have been reconstructed through repeated low-altitude passes, or a household profiled through thermal or nighttime-light data has no practical means of discovering that this has occurred, since there is no transactional trace, no login, no account, and often no publicly available record of which imagery a given operator has captured over a given location. [85]

Even where an individual becomes aware, through litigation disclosure or investigative reporting, that satellite-derived data concerning them has been processed, the remedial pathway is unclear. The Data Protection Board of India, established under the Act, is designed to handle complaints arising from identifiable breaches of specific statutory obligations. [86] It is not evident how a complaint alleging that a commercial EO operator's imagery was used to infer, for instance, unauthorised construction on a person's land or occupancy patterns relevant to a matrimonial or property dispute, would be framed within the Board's existing procedural architecture, since the very act of harm, aggregation and inference from imagery, does not correspond to any of the processing activities the Act was drafted to police. The absence of a workable grievance pathway leaves affected individuals functionally without recourse, notwithstanding the constitutional recognition of informational privacy as a fundamental right. [87]

5.6 Emerging Challenges from AI-Enabled Geospatial Analytics

The regulatory gaps identified above are compounded by the rapid integration of artificial intelligence into geospatial analytics. Machine learning models trained on satellite imagery can now perform automated building detection, vehicle counting, crop health assessment, and, increasingly, human activity recognition, at a scale and speed that manual image interpretation could never achieve. [88] This automation transforms EO data from a passive archival record into an active inferential tool capable of generating new personal data that did not exist in the original imagery at all. [89]

Consider an AI model trained to detect construction activity across a metropolitan region from repeated satellite passes. The model does not merely observe; it infers, flagging a specific plot as likely to belong to an individual engaged in unauthorised construction, or correlating vehicle presence patterns with an individual's likely occupation or income bracket. [90] This is a form of automated decision-making and profiling that closely resembles the concerns Indian and international data protection law seek to address in the context of algorithmic credit scoring or behavioural advertising, yet the DPDP Act contains no provision analogous to the safeguards found in more mature frameworks for automated profiling. [91] Nor does Indian law currently require disclosure of the training data provenance used by commercial EO analytics firms, meaning that imagery of Indian citizens, once licensed, may be used to train models whose outputs are sold back into the Indian market or exported abroad without any statutory checkpoint. [92] The convergence of AI and satellite imagery therefore does not merely aggravate existing gaps, it creates an entirely new category of derivative personal data that the present framework has no vocabulary to describe, let alone regulate.

6. COMPARATIVE PERSPECTIVES ON EARTH OBSERVATION DATA GOVERNANCE

6.1 European Union

The General Data Protection Regulation defines personal data broadly, as any information relating to an identified or identifiable natural person, and this definition has been interpreted by data protection authorities and courts to extend to imagery capable of resolving an individual or their immediate environment. [93] The European Union has, in addition, developed a dedicated Space Programme Regulation and operates its own EO constellation, Copernicus, alongside stringent national security review processes for high-resolution commercial imagery. [94] What distinguishes the European approach is

not a single satellite-specific privacy statute, none exists even in the EU, but the interpretive flexibility of the GDPR itself, which is technology-neutral by design and has been applied, through guidance from national supervisory authorities, to geolocation data, drone imagery, and increasingly to satellite-derived analytics involving identifiable individuals or their property. [95]

The GDPR's emphasis on purpose limitation and data protection impact assessments for high-risk processing gives European regulators a tool that Indian law presently lacks, the ability to require an EO analytics firm to justify, in advance, why a particular processing activity involving identifiable individuals is necessary and proportionate. [96] The EU's approach also benefits from the horizontal application of the right to be forgotten and the right to object, which, while difficult to operationalise for satellite archives just as in India, at least provide a textual hook for litigation that Indian data principals presently lack. [97]

Guidance issued by several national supervisory authorities on drone and geospatial imagery has, moreover, begun to articulate proportionality tests, weighing the resolution of the imagery, the density of population in the area imaged, and the availability of less intrusive alternatives, against the stated commercial or scientific purpose of the processing. [98] India's regulatory instruments contain no equivalent proportionality vocabulary, leaving IN-SPACe's licensing officers to evaluate applications purely against security criteria, with no parallel privacy-oriented checklist to draw upon even if they wished to consider the question.

6.2 United States

The US regulates commercial remote sensing mainly through licensing rather than through data protection law. [99] The Land Remote Sensing Policy Act, and the licensing regime administered by the National Oceanic and Atmospheric Administration control who may operate a high-resolution imaging satellite and under what resolution and shutter-control conditions, principally to protect national security interests, but this licensing tool is silent on the privacy interests of individuals depicted in commercially sold imagery. [100] The US has no detailed federal data protection law comparable to the DPDP Act or the GDPR, and privacy protection for geospatial data is instead scattered across sector-specific statutes, state-level legislation such as the California Consumer Privacy Act, and a body of Fourth Amendment jurisprudence concerned primarily with government, not private, surveillance. [101]

This fragmented landscape means that a commercial EO operator in the United States faces fewer privacy-specific constraints than its counterparts might in Europe, provided it stays within its NOAA licence conditions. [102] The American model is instructive for India chiefly as a cautionary example, licensing-only regulation, focused exclusively on national security and export control, structurally cannot substitute for a data protection regime, because it was never designed to ask whether an individual's privacy interest in their own image or property has been implicated at all.

6.3 Canada

Canada's Remote Sensing Space Systems Act establishes a licensing regime for satellite operators broadly similar to the American model, administered with attention to national security, foreign policy, and international obligations. [103] Canada additionally benefits from the Personal Information Protection and Electronic Documents Act, which, like the GDPR, applies a broad and technology-neutral definition of personal information capable, in principle, of extending to identifiable satellite imagery, although Canadian courts and the Office of the Privacy Commissioner have not yet generated a substantial body of interpretive guidance specific to EO data. [104]

What is notable about the Canadian model is the degree of coordination it attempts between the space licensing authority and general privacy oversight, even though this coordination remains largely informal and untested through litigation. Licence conditions issued under the Remote Sensing Space Systems Act require operators to maintain a system safety and control regime, but privacy considerations enter, if at all, only indirectly, through the general applicability of federal privacy legislation to any commercial entity collecting information in the course of its business. [105] There is no requirement, comparable to what this article proposes for India, that an applicant demonstrate privacy safeguards specific to the imaging activity itself as a condition of licence approval. [106]

For India, the Canadian experience underscores that even jurisdictions with comparatively mature space and privacy statutes have not yet produced a dedicated EO-specific privacy framework, reinforcing the argument that this is a genuinely emerging regulatory frontier rather than a problem India has simply failed to keep pace with.

6.4 Lessons for India's Regulatory Framework

Three lessons emerge from this comparative survey. First, no major jurisdiction currently possesses a satellite-specific data protection statute, which means India has an opportunity, rather than a deficiency relative to peers, in building one from first principles rather than retrofitting an existing model. Second, the European experience demonstrates the value of a broad, technology-neutral definition of personal data combined with risk-based obligations such as impact assessments, an approach India's DPDP Act could adopt through subordinate legislation or sectoral rules without requiring a wholesale statutory amendment. Third, the American and Canadian experience demonstrates the limits of licensing-only regulation, confirming that IN-SPACe's authorisation framework, however well suited to its national security objectives, cannot by itself discharge the function of a data protection regime, and that India's forthcoming space legislation must therefore be drafted in conscious coordination with, rather than as a substitute for, the DPDP Act.

7. TOWARDS A DEDICATED REGULATORY FRAMEWORK FOR SATELLITE-DERIVED GEOSPATIAL DATA IN INDIA

7.1 Need for a Specialised Legal Framework

The preceding analysis demonstrates that neither the DPDP Act nor India's space governance instruments, taken alone or together, adequately address the privacy implications of contemporary Earth Observation. This is not an argument for discarding either framework, but for building a bridge between them. A specialised framework is necessary because satellite-derived data possesses characteristics, passive collection without any point of individual interaction, inherent capacity for retrospective and predictive inference, and a multi-tiered commercial value chain, that general-purpose data protection law was not designed to address. [107] Waiting for litigation to force an interpretive extension of the DPDP Act risks years of regulatory uncertainty during precisely the period in which India's commercial EO sector is scaling most rapidly under IN-SPACe. [108]

7.2 Defining Satellite-Derived Personal Data

Any workable framework must begin with a definition. Satellite-derived personal data may be defined as any geospatial information, whether raw imagery or a product derived through processing, enhancement, or algorithmic analysis of such imagery, that relates to an identified or identifiable individual, or to property or premises reasonably associated with an identifiable individual, including where such identifiability arises only through combination with other available datasets. This definition deliberately captures the mosaic effect, the possibility that innocuous imagery becomes identifying only once combined with land records, utility data, or social media geotags, since a definition confined to directly identifying imagery alone would exclude the majority of realistic privacy harms in this domain. [109]

7.3 Obligations of Earth Observation Operators

Operators falling within this definition should be subject to graduated obligations calibrated to resolution and processing intensity rather than a uniform compliance burden. At minimum, operators dealing in sub-metre resolution imagery of inhabited areas should be required to conduct a data protection impact assessment prior to large-scale commercial deployment, to maintain records of onward licensing sufficient to trace an image from capture to end use, and to establish a defined retention and deletion policy rather than indefinite archival by default. [110] Obligations should also extend to disclosure requirements where imagery is used to train or fine-tune AI models, given the derivative personal data concerns identified in Part 5.6, so that model developers cannot escape accountability simply because the output of the model, rather than the imagery itself, is what ultimately identifies an individual. [111]

7.4 Regulatory Oversight and Institutional Mechanisms

Institutional design should avoid creating an entirely new regulator, which would risk further fragmentation. Instead, a coordination mechanism between IN-SPACe and the Data Protection Board of India is preferable, under which IN-SPACe's existing authorisation process is amended to require applicants to demonstrate baseline data protection compliance as a precondition of licensing, while the Data Protection Board retains jurisdiction over complaints and enforcement once an operator is licensed. [112] This avoids duplicative institutional capacity-building while ensuring that data protection considerations enter the regulatory conversation at the point of licensing, rather than only after harm has already occurred and been discovered.

A practical mechanism for this coordination could take the form of a standing memorandum of understanding between the Department of Space and the Ministry of Electronics and Information Technology, under which IN-SPACe forwards a copy of each authorisation application involving sub-metre resolution imaging capability to the Data Protection Board for a non-binding advisory opinion, to be issued within a fixed statutory timeline so as not to delay commercial licensing unduly. Such a mechanism would allow privacy concerns to inform licensing decisions without requiring the Board to develop parallel technical expertise in satellite engineering, since IN-SPACe would remain the primary technical regulator while the Board contributes the privacy-specific lens that IN-SPACe's existing mandate does not equip it to apply. [113]

7.5 Integrating the DPDP Act with Future Indian Space Legislation

India's anticipated comprehensive space legislation, intended to replace the current patchwork of executive norms and authorisation guidelines, presents a rare legislative window. [114] That statute should expressly cross-reference the DPDP Act's definitions and obligations rather than developing a freestanding and potentially inconsistent privacy vocabulary of its own. Express cross-referencing would ensure that satellite-derived personal data is treated, for enforcement purposes, as a species of personal data generally, subject to sector-specific supplementary obligations, rather than as a wholly separate category adjudicated under an entirely different statutory logic. [115] This integration is achievable at the drafting stage with comparatively modest legislative effort, since it requires coordination between the Department of Space and the Ministry of Electronics and Information Technology rather than the creation of new substantive rights.

7.6 Proposed Regulatory Model

Drawing the preceding recommendations together, the proposed model rests on four elements: a statutory definition of satellite-derived personal data incorporating the mosaic effect, graduated operator obligations tied to resolution and processing intensity, a coordination mechanism linking IN-SPACe licensing with Data Protection Board enforcement, and express integration of this framework into India's forthcoming space legislation. This model is deliberately incremental. It does not propose a standalone Earth Observation privacy statute, which would risk regulatory duplication and delay, but a set of targeted amendments and coordination mechanisms capable of being implemented within the existing institutional architecture, while leaving room for more comprehensive treatment once India's space legislation is finalised and a body of enforcement experience under the DPDP Act itself has developed.

8. CONCLUSION

Earth Observation technology has moved far faster than the legal instruments meant to govern it. The UN Principles of 1986 were made for a world of state-operated reconnaissance satellites and it could not have anticipated a commercial market place which is capable of near real-time, AI-enhanced imaging of individual rooftops and vehicles. India's Digital Personal Data Protection Act, 2023, for all its significance as the country's first comprehensive data protection statute, have the same blind spot, built for data flows, it offers no space for passive, orbital collection of information about people who will never knew why they were being observed. The comparative analysis done in this research confirms that this is not a uniquely Indian failing; no major jurisdiction has yet produced a satellite-specific privacy framework. That, however, is precisely why India's position is significant. With its commercial EO sector expanding rapidly under IN-SPACe and a comprehensive space legislation still on the horizon, India have a narrow but real opportunity to fill this gap deliberately, through defined categories, calibrated obligations, and coordinated institutional oversight, instead of waiting for the gap to be exposed through various litigation after the harm has already occurred. The legal framework proposed in this article is modest by design, but its central claim is not: satellite-derived personal data must be named, classified, and regulated as such, before India's Earth Observation ecosystem outgrows the legal categories meant to contain it.

REFERENCES

- [1] Jakhu RS, Pelton JN, editors. Global space governance: an international study. Cham: Springer; 2017. p. 323-39.
- [2] Williamson RA, Baker JC. Commercial observation satellites: at the leading edge of global transparency. Santa Monica: RAND Corporation; 2001. p. 11-39.
- [3] United Nations Office for Outer Space Affairs. Space supporting the sustainable development goals. Vienna: United Nations; 2018
- [4] Gabrynowicz JI. The perils of Landsat from grassroots to globalization: a comprehensive review of US remote sensing law with a few thoughts for the future. J Air Law Commer 2003;48:589-606.

- [5] Chuvieco E. *Fundamentals of satellite remote sensing: an environmental approach*. 3rd ed. Boca Raton: CRC Press; 2020. p. 1-18.
- [6] Richards JA. *Remote sensing digital image analysis: an introduction*. 6th ed. Cham: Springer; 2022. p. 37-61.
- [7] OECD. *The space economy in figures: how space contributes to the global economy*. Paris: OECD Publishing; 2019. p. 169-82.
- [8] Jensen JR. *Remote sensing of the environment: an earth resource perspective*. 2nd ed. Upper Saddle River: Pearson Prentice Hall; 2007. p. 8-17; European Space Agency. *SPOT and European earth observation missions*. Noordwijk: ESA Publications Division; 2020.
- [9] Land Remote Sensing Policy Act of 1992, Pub L No 102-555, 106 Stat 4163. 1992; Gabrynowicz JI. The perils of Landsat from grassroots to globalization: a comprehensive review of US remote sensing law with a few thoughts for the future. *J Air Law Commer* 2003;48:566-90.
- [10] U.S. Commercial Space Launch Competitiveness Act, Pub L No 114-90, 129 Stat 704. 2015; Jakhu RS, Pelton JN, editors. *Global space governance: an international study*. Cham: Springer; 2017. p. 337-45.
- [11] Regulation (EU) No. 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus programme and repealing Regulation (EU) No. 911/2010, 2014 OJ (L 122):44; European Commission. *Copernicus: Europe's eyes on Earth*. Luxembourg: Publications Office of the European Union; 2022.
- [12] OECD. *The space economy in figures: how space contributes to the global economy*. Paris: OECD Publishing; 2019. p. 169-84; BryceTech. *State of the satellite industry report*. Alexandria (VA): Satellite Industry Association; 2023.
- [13] European Space Agency. *Artificial intelligence for earth observation*. Noordwijk: ESA Φ-lab; 2023; Lary DJ, et al. *Machine learning in geosciences and remote sensing*. *Geosci Front* 2016;8:13-27.
- [14] OECD. *Artificial intelligence, machine learning and big data in the space sector*. Paris: OECD Space Forum; 2022; Floridi L. *The ethics of artificial intelligence*. Oxford: Oxford University Press; 2023. p. 173-98.
- [15] Principles relating to remote sensing of the Earth from outer space, GA Res 41/65, UN Doc A/RES/41/65. 1986 Dec 3; Gabrynowicz JI. Remote sensing and the growing challenge of commercial satellite imagery. *J Space Law* 2007;33:150-67.
- [16] European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art 4(1). 2016 OJ (L 119):1; Schwartz PM, Solove DJ. *Information privacy law*. 7th ed. New York: Wolters Kluwer; 2021. p. 83-105.
- [17] Article 29 Data Protection Working Party. Opinion 05/2014 on anonymisation techniques, WP216. 2014 Apr 10; Finck M, Pallas F. They who must not be identified—distinguishing personal from non-personal data under the GDPR. *Int Data Privacy Law* 2020;10:18-30.
- [18] Wachter S, Mittelstadt B. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum Bus Law Rev* 2019;494:520-60; European Data Protection Board. *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*. Version 2.0. 2021 Mar 9.
- [19] Richards NM. *The dangers of surveillance*. Cambridge (MA): Harvard University Press; 2015. p. 19-46; Solove DJ. *Understanding privacy*. Cambridge (MA): Harvard University Press; 2008. p. 92-118.
- [20] Richards NM. *The dangers of surveillance*. Cambridge (MA): Harvard University Press; 2015. p. 19-46; Solove DJ. *Understanding privacy*. Cambridge (MA): Harvard University Press; 2008. p. 92-118.
- [21] Williamson RA, Baker JC. *Commercial observation satellites: at the leading edge of global transparency*. Santa Monica: RAND Corporation; 2001. p. 75-98; Secure World Foundation. *Global counterspace capabilities: an open source assessment*. 2024 ed. Broomfield: Secure World Foundation; 2024. p. 37-61.
- [22] Richards NM. *Intellectual privacy: rethinking civil liberties in the digital age*. New York: Oxford University Press; 2015. p. 89-117; United Nations Human Rights Council. *The right to privacy in the digital age*. UN Doc A/HRC/39/29. 2018 Aug 3. p. 8-16.
- [23] United Nations Office for Outer Space Affairs. *United Nations treaties and principles on outer space*. Vienna: United Nations; 2008. p. 43-46; Gabrynowicz JI. The UN principles relating to remote sensing of the Earth from outer space: a review. *J Space Law* 2007;33:113-19.
- [24] Cheng B. *Studies in international space law*. Oxford: Clarendon Press; 1997. p. 589-608; Tronchetti F. *Fundamentals of space law and policy*. New York: Springer; 2013. p. 145-50.

- [25] Principles relating to remote sensing of the Earth from outer space. GA Res 41/65. UN Doc A/RES/41/65. 1986 Dec 3.
- [26] Jakhu RS, Pelton JN, editors. Global space governance: an international study. Cham: Springer; 2017. p. 209-20; von der Dunk FG, Tronchetti F, editors. Handbook of space law. Cheltenham: Edward Elgar Publishing; 2015. p. 533-
- [27] Treaty on principles governing the activities of States in the exploration and use of outer space, including the Moon and other celestial bodies. 610 UNTS 205. 1967 Jan 27. Entered into force 1967 Oct 10. art I.
- [28] Cheng B. Studies in international space law. Oxford: Clarendon Press; 1997. p. 589-622; Gabrynowicz JI. The UN principles relating to remote sensing of the Earth from outer space: a review. J Space Law 2007;33:120-29.
- [29] Outer Space Treaty. art II; Gorove S. Developments in space law: issues and policies. Dordrecht: Martinus Nijhoff Publishers; 1991. p. 115-28.
- [30] Tronchetti F. Fundamentals of space law and policy. New York: Springer; 2013. p. 145-53; von der Dunk FG, Tronchetti F, editors. Handbook of space law. Cheltenham: Edward Elgar Publishing; 2015. p. 533-48.
- [31] Regulation (EU) No. 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus programme and repealing Regulation (EU) No. 911/2010. 2014 OJ (L 122):44; European Commission. Copernicus data policy: free, full and open access to Copernicus data and information. Brussels: European Commission.
- [32] Land Remote Sensing Policy Act of 1992, Pub L No 102-555, 106 Stat 4163. 1992; 15 CFR pt 960. Licensing of private remote sensing space systems; National Oceanic and Atmospheric Administration. Commercial remote sensing regulatory affairs (CRSRA).
- [33] Gabrynowicz JI. The UN principles relating to remote sensing of the Earth from outer space: a review. J Space Law 2007;33:123-31; von der Dunk FG, Tronchetti F, editors. Handbook of space law. Cheltenham: Edward Elgar Publishing; 2015. p. 533-48.
- [34] Indian Space Research Organisation. Earth observation satellites [Internet]. Department of Space, Government of India. [cited 2026 Aug 8]. Available from: <https://www.isro.gov.in>
- [35] Indian National Space Promotion and Authorization Centre. IN-SPACe selects consortium led by Pixxel, Dhruva Space, PierSight and SatSure for India's first private Earth observation constellation under PPP model [press release]. 2025 Aug; Department of Space, Government of India.
- [36] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023); Department of Space, Government of India. Indian space policy, 2023.
- [37] Indian National Space Promotion and Authorisation Centre. About IN-SPACe [Internet]. Department of Space, Government of India. [cited 2026 Aug 8]. Available from: <https://www.inspace.gov.in>
- [38] Department of Space, Government of India. Indian space policy, 2023. p. 7-10.
- [39] Department of Space, Government of India. Indian space policy, 2023; Government of India. Draft space activities bill, 2017 [draft, not enacted].
- [40] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023); Department of Space, Government of India. Indian space policy, 2023.
- [41] Department of Science and Technology, Government of India. Guidelines for acquiring and producing geospatial data and geospatial data services including maps. 2021 Feb 15; Department of Science and Technology, Government of India. National geospatial policy, 2022.
- [42] Guidelines for acquiring and producing geospatial data and geospatial data services including maps. 2021. cls 3-6.
- [43] Department of Science and Technology, Government of India. National geospatial policy, 2022; Department of Science and Technology, Government of India. Guidelines for acquiring and producing geospatial data and geospatial data services including maps, 2021.
- [44] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
- [45] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), § 2(t).
- [46] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), § 2(t); Justice KS Puttaswamy (Retd.) v Union of India. 2017;10 SCC 1.
- [47] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), § 2(t); Justice KS Puttaswamy (Retd.) v Union of India. 2017;10 SCC 1.

- [48] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts 13-14; Voigt P, von dem Bussche A. The EU General Data Protection Regulation (GDPR): a practical guide. 2nd ed. Cham: Springer; 2023. p. 120-32.
- [49] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), § 2(t).
- [50] Justice KS Puttaswamy (Retd.) v Union of India. 2017;10 SCC 1; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art 4(1).
- [51] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
- [52] Regulation (EU) 2016/679 (General Data Protection Regulation), recital 26; European Data Protection Board. Opinion 05/2014 on anonymisation techniques. WP216. 2014. p. 8-14.
- [53] Justice KS Puttaswamy (Retd.) v Union of India. 2017;10 SCC 1.
- [54] Justice KS Puttaswamy (Retd.) v Union of India. 2017;10 SCC 1. p. 180, 310, 325-27.
- [55] Justice KS Puttaswamy (Aadhaar-5J.) v Union of India. 2019;1 SCC 1. p. 442-47, 449-51.
- [56] People's Union for Civil Liberties (PUCL) v Union of India. 1997;1 SCC 301.
- [57] Department of Science and Technology, Government of India. National geospatial policy, 2022; Indian National Space Promotion and Authorisation Centre. Norms, guidelines and procedures for authorisation of space activities, as amended.
- [58] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), § 2(t).
- [59] Ministry of Electronics and Information Technology, Government of India. Explanatory note on the Digital Personal Data Protection Act, 2023; Greenleaf G. Asian data privacy laws: trade and human rights perspectives. Oxford: Oxford University Press; 2014. p. 505-12.
- [60] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023); Department of Space, Government of India. Indian space policy, 2023 [Internet]. [cited 2026 Jul 21]. Available from: <https://www.isro.gov.in/IndianSpacePolicy2023.html>.
- [61] Digital Personal Data Protection Act, 2023; Digital Personal Data Protection Rules, where applicable; Department of Space, Government of India. Indian space policy, 2023.
- [62] Vincent N, Li H, Hecht B. The privacy implications of satellite imagery in the era of artificial intelligence. Nat Mach Intell. 2024; European Data Protection Board. Guidelines 3/2019 on processing of personal data through video devices.
- [63] Digital Personal Data Protection Act, 2023; Schwartz PM, Solove DJ. Information privacy law. 7th ed. New York: Wolters Kluwer; 2021. p. 66-81.
- [64] Department of Space, Government of India. Indian space policy, 2023; Indian National Space Promotion and Authorization Centre. Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Internet]. [cited 2026 Jul 5]. Available from: <https://www.inspace.gov.in>.
- [65] Department of Space, Government of India. Indian space policy, 2023; Government of India. Draft space activities bill, 2017; Jakhu RS, editor. National regulation of space activities. Dordrecht: Springer; 2010. p. 193-211.
- [66] Justice KS Puttaswamy (Retd.) v Union of India. 2017;10 SCC 1. p. 297-307, 325.
- [67] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), §§ 4-6.
- [68] Digital Personal Data Protection Act, 2023, §§ 4-6; Ministry of Electronics and Information Technology, Government of India. Frequently asked questions on the Digital Personal Data Protection Act, 2023 [Internet]. [cited 2026 Jul 21]. Available from: <https://www.meity.gov.in>.
- [69] National Geospatial-Intelligence Agency. Commercial remote sensing and geospatial intelligence overview [Internet]. [cited 2026 Jul 21]. Available from: <https://www.nga.mil>; European Space Agency. Earth observation applications [Internet]. [cited 2026 Jul 21]. Available from: <https://www.esa.int>.
- [70] Digital Personal Data Protection Act, 2023, § 7.
- [71] Digital Personal Data Protection Act, 2023, §§ 6-7; Greenleaf G. Asian data privacy laws: trade and human rights perspectives. Oxford: Oxford University Press; 2014. p. 511-18.
- [72] European Data Protection Board. Guidelines 01/2024 on the processing of personal data through drones; European Union Aviation Safety Agency. Drone operations and data protection [Internet]. [cited 2026 Jul 21]. Available from: <https://www.easa.europa.eu>; Wood DM. Surveillance studies: a reader. Maidenhead: Open University Press; 2018. p. 289-302.
- [73] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), §§ 2(i), 2(z), 8-9.
- [74] Indian National Space Promotion and Authorization Centre. Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Internet]. [cited 2026 Jul 21]. Available from: <https://www.inspace.gov.in>; Department of

- Space, Government of India. Indian space policy, 2023; Organisation for Economic Co-operation and Development. The space economy in figures: how space contributes to the global economy. Paris: OECD Publishing; 2019.
- [75] European Space Agency. EO handbook: earth observation applications and value chain [Internet]. [cited 2026 Jul 21]. Available from: <https://earth.esa.int>; Organisation for Economic Co-operation and Development. Space economy in figures. Paris: OECD Publishing; 2019.
- [76] Digital Personal Data Protection Act, 2023, §§ 2(i), 2(z), 8-9; Schwartz PM, Solove DJ. Information privacy law. 7th ed. New York: Wolters Kluwer; 2021. p. 168-82.
- [77] Indian National Space Promotion and Authorization Centre. Norms, guidelines and procedures for implementation of Indian space policy, 2023; Department of Space, Government of India. Indian space policy, 2023 [Internet]. [cited 2026 Jul 21]. Available from: <https://www.isro.gov.in/IndianSpacePolicy2023.html>.
- [78] Indian National Space Promotion and Authorization Centre. Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Internet]. [cited 2026 Jul 21]; Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
- [79] European Space Agency. Ground segment and Earth observation data processing [Internet]. [cited 2026 Jul 21]. Available from: <https://earth.esa.int>; Organisation for Economic Co-operation and Development. The space economy in figures. Paris: OECD Publishing; 2019.
- [80] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), § 16; Regulation (EU) 2016/679 (General Data Protection Regulation), arts 44-49.
- [81] United Nations Office for Outer Space Affairs. Space supporting the sustainable development goals [Internet]. [cited 2026 Jul 21]. Available from: <https://www.unoosa.org>; Jakhu RS, Pelton JN, editors. Global space governance. Cham: Springer; 2017. p. 419-35.
- [82] Department of Space, Government of India. Indian space policy, 2023; Indian National Space Promotion and Authorization Centre. Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Internet]. [cited 2026 Jul 21]. Available from: <https://www.inspace.gov.in>.
- [83] Digital Personal Data Protection Act, 2023, § 8; Regulation (EU) 2016/679 (General Data Protection Regulation), art 5(1)(e); Schwartz PM, Solove DJ. Information privacy law. 7th ed. New York: Wolters Kluwer; 2021. p. 266-73.
- [84] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), §§ 11-15.
- [85] European Data Protection Board. Guidelines 3/2019 on processing of personal data through video devices; European Space Agency. Earth observation applications [Internet]. [cited 2026 Jul 21]. Available from: <https://www.esa.int>.
- [86] Digital Personal Data Protection Act, 2023, §§ 18-27.
- [87] Justice KS Puttaswamy (Retd.) v Union of India. 2017;10 SCC 1. p. 297-307, 325; Digital Personal Data Protection Act, 2023, §§ 11-27.
- [88] European Space Agency. Artificial intelligence for Earth observation [Internet]. [cited 2026 Jul 21]. Available from: <https://www.esa.int>; National Aeronautics and Space Administration. Artificial intelligence and Earth science data systems [Internet]. [cited 2026 Jul 21]. Available from: <https://www.nasa.gov>; Lary DJ, et al. Machine learning in geosciences and remote sensing. Geosci Front. 2016;3:3-10.
- [89] Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun. 2019;10:3069; Schwartz PM, Solove DJ. Information privacy law. 7th ed. New York: Wolters Kluwer; 2021. p. 67-82.
- [90] Weng Q. Remote sensing for urban intelligence: AI, machine learning and geospatial analytics. Boca Raton: CRC Press; 2023. p. 45-68; European Space Agency. Earth observation and artificial intelligence [Internet]. [cited 2026 Jul 21]. Available from: <https://earth.esa.int>.
- [91] Regulation (EU) 2016/679 (General Data Protection Regulation), arts 22, 35; Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023); Wachter S, Mittelstadt B, Floridi L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. Int Data Priv Law. 2017;7:76-99.
- [92] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023); Organisation for Economic Co-operation and Development. OECD framework for the classification of AI systems. 2022; UNESCO. Recommendation on the ethics of artificial intelligence [Internet]. 2021 [cited 2026 Jul 21]. Available from: <https://www.unesco.org>.
- [93] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art 4(1), recital 26; Court of Justice of the European Union. Patrick Breyer v Bundesrepublik Deutschland.

- Case C-582/14. ECLI:EU:C:2016:779; European Data Protection Board. Guidelines 01/2020 on processing personal data in connected vehicles.
- [94] Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme. 2021 OJ (L 170):69; European Commission. Copernicus: Europe's Earth observation programme [Internet]. [cited 2026 Jul 21]. Available from: <https://www.copernicus.eu>.
 - [95] Regulation (EU) 2016/679 (General Data Protection Regulation), recitals 15, 26, arts 4-5; European Data Protection Board. Guidelines 3/2019 on processing of personal data through video devices; European Data Protection Supervisor. TechDispatch on remote sensing and privacy [Internet]. [cited 2026 Jul 21]. Available from: <https://www.edps.europa.eu>.
 - [96] Regulation (EU) 2016/679 (General Data Protection Regulation), arts 5(1)(b), 35-36; Voigt P, von dem Bussche A. The EU General Data Protection Regulation (GDPR): a practical guide. 2nd ed. Cham: Springer; 2022. p. 211-39.
 - [97] Regulation (EU) 2016/679, arts. 17, 21; Lynskey O. The foundations of EU data protection law. Oxford: Oxford University Press; 2015. p. 274-302.
 - [98] French Data Protection Authority (CNIL). Drones: respecting privacy [Online]. [cited 2026 Jul 21]. Available from: <https://www.cnil.fr>; Spanish Data Protection Agency (AEPD). Guidelines on the use of drones [Online]. [cited 2026 Jul 21]. Available from: <https://www.aepd.es>; European Data Protection Board. Guidelines 3/2019 on processing of personal data through video devices.
 - [99] Land Remote Sensing Policy Act of 1992, 51 U.S.C. §§ 60101-60126; National Oceanic and Atmospheric Administration (NOAA). Commercial remote sensing regulatory affairs [Online]. [cited 2026 Jul 21]. Available from: <https://www.nesdis.noaa.gov/commercial-remote-sensing-regulatory-affairs>.
 - [100] 15 C.F.R. pt. 960. Licensing of private remote sensing space systems; National Oceanic and Atmospheric Administration (NOAA). Commercial remote sensing licensing guidance [Online]. [cited 2026 Jul 21]. Available from: <https://www.nesdis.noaa.gov>; Land Remote Sensing Policy Act of 1992, 51 U.S.C. §§ 60121-60125.
 - [101] California Consumer Privacy Act of 2018, Cal Civ Code §§ 1798.100-1798.199; Carpenter v United States, 585 US 296 (2018); Solove DJ, Schwartz PM. Information privacy law. 7th ed. New York: Wolters Kluwer; 2021. p. 1127-1178.
 - [102] National Oceanic and Atmospheric Administration (NOAA), *Commercial Remote Sensing Regulatory Affairs*, available at: <https://www.nesdis.noaa.gov/commercial-remote-sensing-regulatory-affairs> (Visited on July 21, 2026); Scott Pace, *The U.S. Commercial Remote Sensing Industry and National Security*, 37 *Space Policy* 1-9 (2016).
 - [103] Remote Sensing Space Systems Act, SC 2005, c 45 (Canada), ss. 5-8; Government of Canada. Remote sensing space systems act [Online]. [cited 2026 Jul 21]. Available from: <https://laws-lois.justice.gc.ca>.
 - [104] Personal Information Protection and Electronic Documents Act, SC 2000, c 5, ss. 2, 5; Office of the Privacy Commissioner of Canada. PIPEDA in brief [Online]. [cited 2026 Jul 21]. Available from: <https://www.priv.gc.ca>; Bennett CJ, Raab CD. The governance of privacy: policy instruments in global perspective. 2nd ed. Cambridge: MIT Press; 2006.
 - [105] Remote Sensing Space Systems Regulations, SOR/2007-66 (Canada), pts. 2, 3; Remote Sensing Space Systems Act, SC 2005, c 45.
 - [106] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5; Office of the Privacy Commissioner of Canada, *Guidance on Privacy Impact Assessments*, available at: <https://www.priv.gc.ca> (Visited on July 21, 2026); *Remote Sensing Space Systems Act*, S.C. 2005, c. 45.
 - [107] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023); Department of Space, Government of India. Indian space policy 2023; Indian National Space Promotion and Authorization Centre (IN-SPACe). Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Online]. [cited 2026 Jul 21]. Available from: <https://www.inspace.gov.in>; Greenleaf G. Asian data privacy laws: trade and human rights perspectives. Oxford: Oxford University Press; 2021.
 - [108] Department of Space, Government of India. Indian space policy 2023; Indian National Space Promotion and Authorization Centre (IN-SPACe). Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Online]. [cited 2026 Jul 21]. Available from: <https://www.inspace.gov.in>; Organisation for Economic Co-operation and Development (OECD). The space economy in figures. Paris: OECD Publishing; 2019.
 - [109] Regulation (EU) 2016/679 (General Data Protection Regulation), art. 4(1), recital 26; Justice K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1; European Union Agency for Cybersecurity (ENISA). Pseudonymisation techniques and

- best practices. 2021; Schwartz PM, Solove DJ. Information privacy law. 7th ed. New York: Wolters Kluwer; 2021. p. 67-82.
- [110] Regulation (EU) 2016/679, arts. 5(1)(e), 30, 35; The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), s. 8; European Data Protection Board. Guidelines 4/2019 on Article 25 data protection by design and by default; Indian National Space Promotion and Authorization Centre (IN-SPACe). Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Online]. [cited 2026 Jul 21]. Available from: <https://www.inspace.gov.in>.
- [111] UNESCO. Recommendation on the ethics of artificial intelligence. 2021 [Online]. [cited 2026 Jul 21]. Available from: <https://www.unesco.org>; Organisation for Economic Co-operation and Development (OECD). OECD framework for the classification of AI systems. 2022; Regulation (EU) 2016/679, arts. 5, 13, 35; European Commission. Ethics guidelines for trustworthy AI. 2019.
- [112] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), ss. 18-27; Department of Space, Government of India. Indian space policy 2023; Indian National Space Promotion and Authorization Centre (IN-SPACe). Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Online]. [cited 2026 Jul 21]. Available from: <https://www.inspace.gov.in>.
- [113] Department of Space, Government of India. Indian space policy 2023; The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), ss. 18-27; Organisation for Economic Co-operation and Development (OECD). Recommendation of the Council on digital government strategies. 2014; Organisation for Economic Co-operation and Development (OECD). OECD regulatory policy outlook 2021. Paris: OECD Publishing; 2021.
- [114] Department of Space, Government of India. Indian space policy 2023; Indian National Space Promotion and Authorization Centre (IN-SPACe). Norms, guidelines and procedures for implementation of Indian space policy, 2023 [Online]. [cited 2026 Jul 21]. Available from: <https://www.inspace.gov.in>; Government of India, Department of Space. Draft national space legislation (policy discussions and legislative proposals).
- [115] Theal Personal Data Protection Act, 2023 (Act No. 22 of 2023), ss. 2(t), 2(i), 2(z), 8–15 & 18–27; Department of Space, Government of India, *Indian Space Policy – 2023*; Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press, Oxford, 2021).