THE TECH LAW GUIDE FOR STARTUPS

Where emerging technology meets real-world law

1st Edition [2026]- Theory and Practice

Building a startup in tech today means navigating law that is still catching up.

This guide is written from the ground up for founders, operators, and in-house teams who are actually building.

Inside, you'll find a practical take on AI, crypto, Web3, space law, technology contracts, and disputes in India. The focus is simple- what matters, what can go wrong, and how to deal with it before it becomes expensive.

No abstract frameworks without context, no legal jargon for the sake of it. Just how things play out in the real world.

By Chandan Goswami

Partner, AT & Partners

Important notice

This guide is intended for general informational purposes only. It does not constitute legal advice and should not be relied upon as such. The law in these areas is rapidly evolving. Founders and companies are encouraged to seek specific legal counsel before making decisions. The author and AT & Partners accept no liability for any action taken in reliance on this material.

New Delhi
C-585, LGF, Defence Colony
New Delhi-110024
+91-8318933044

Also present in
Jabalpur| Lucknow| Odisha| Mumbai|
www.atandpartners.in
office@atandpartners.in

INDEX

ABOUT THE FIRM

The firm was built on a fairly simple idea. The most important legal questions going forward won't sit neatly within traditional boundaries. They will come up where law meets technology and lawyers working on those problems need to be comfortable with both. That's where the practice is focused. Artificial intelligence, blockchain and cryptocurrency, Web3, space law, technology contracts. Areas where the law is still evolving, and the consequences are real.

Alongside this sits a full-service corporate and commercial litigation practice because advisory work changes when you've seen how things fall apart in court and litigation is sharper when you actually understand the business and commercial logic behind the dispute.

"Law firms that do not understand technology will spend the next decade being surprised by it. We chose a different path."

- Anusha Soni, Managing Partner

RESEARCH AS THE FOUNDATION OF PRACTICE

At AT & Partners, research is not a support function but the foundation of the practice. The firm's approach to each area of law it advises on begins with a commitment to understanding the legal landscape more thoroughly than any counterpart across the table. In technology law, where the regulatory framework is often unsettled, where statutes are drafted years after the technology they govern has already matured, and where the consequences of legal uncertainty fall directly on the companies navigating it, that commitment is not optional.

The firm publishes regularly on the legal questions that matter most to its clients as a discipline. Writing forces precision and precision produces better advice. The publications that emerge from the firm's research reflect in its client work i.e. accurate, specific, and useful.

AREAS OF PRACTICE

Artificial Intelligence

AI governance frameworks, liability for AI errors, IP ownership in AI-generated outputs, AI contract structuring, EU AI Act compliance for India-based companies, and advisory on AI deployment in regulated sectors including financial services, healthcare, and insurance.

Cryptocurrency & Blockchain

Token structuring and regulatory classification, exchange compliance and FIU-IND registration, AML/KYC programme design, DAO frameworks, jurisdictional regulatory navigation, and representation in crypto-related regulatory inquiries.

Web3 & Digital Assets

Platform documentation and IP frameworks, smart contract legal structures, DeFi regulatory advisory, digital asset transaction documentation, deal structuring, hack response and recovery.

Space Law

IN-SPACe authorisation and engagement, advisory under the Indian Space Policy 2023 and NGP 2024, remote sensing data commercialisation under RSDP 2011, insurance structuring for space activities, and international space treaty implications for private operators.

Technology Contracts

SaaS and technology services agreements, AI-specific contract provisions, software development and IP assignment, DPDP Act compliance in commercial agreements, data processing agreements, and procurement contracts for technology companies.

Corporate & Commercial Litigation

Technology sector disputes, commercial arbitration, contract disputes, IP litigation, regulatory enforcement response, and crisis management across sectors including technology, FMCG, petroleum, and financial services.

GEOGRAPHIC PRACTICE

The firm's base of operations is New Delhi. Partners and senior counsel are regularly present in Dubai, Singapore, London, Bangalore, Hyderabad, and Kolkata. The firm advises clients in Singapore, London, UAE, Panama, and the United States.

PUBLICATIONS & THOUGHT LEADERSHIP

The firm publishes in several formats, reflecting the different purposes that publishing serves in a serious legal practice.

Research guides are the firm's flagship publications. Written to the standard of a practitioner's reference, they address areas of law that clients most need to understand and that most existing commentary addresses inadequately. The Tech Law Guide for Startups, published annually, is the firm's primary reference publication.

Regulatory updates are published when significant legal or regulatory developments require immediate analysis. These are written for clients and counterparts who need to understand what has changed and what it means in practice and not just a summary of what was announced, but an assessment of what it requires.

Opinion and analysis pieces are published in The Hindu, Mint, and other publications. These represent the firm's considered view on significant legal questions written to inform the broader public debate, not to generate instructions.

ON THE PRACTICE OF TECHNOLOGY LAW

"The law is always catching up. The question is whether you are ahead of where the law is going, or behind where it already is."

Chandan Goswami, Partner

The technology sector is building at a pace that the legal infrastructure is not always equipped to support. Regulations are introduced years after the industries they govern have matured and Courts are tasked to apply legal doctrines developed for a different economic era to disputes that arise from technologies those doctrines never contemplated. The regulatory bodies that will shape the next decade of technology law in India i.e. MeitY, SEBI, RBI, IN-SPACe, the Data Protection Board are in various stages of operationalisation, and the frameworks they are building will have consequences that are not yet fully visible.

AT & Partners was established to operate in that environment; not to wait for certainty before advising, but to provide counsel that is calibrated to the genuine state of the law and honest about its uncertainties. The firm's clients are companies and individuals who are building in areas where the legal terrain is still being mapped. The value the firm provides is not the comfort of a settled answer, but the clarity of the most accurate answer available and the capability to defend it.

PARTNER's PROFILE

Chandan Goswami is a Partner at AT & Partners, where he leads the firm's technology law practice. He has more than a decade of experience advising companies, founders, institutions, and private clients on legal matters arising at the intersection of technology and law; from the structuring of cryptocurrency exchanges and the drafting of AI deployment agreements, to the management of complex commercial disputes in sectors including technology, petroleum, FMCG, and financial services.

Goswami's practice reflects a sustained focus on the areas of law where the rate of technological change most consistently outpaces the development of legal frameworks. He has advised on matters arising under the Prevention of Money Laundering Act as it applies to virtual asset service providers, on the structuring of token issuances, on hack recovery and response, on cryptocurrency and digital assets recovery, on various web3 legal frameworks, on AI contract provisions governing IP ownership and liability, and on the regulatory framework governing private participation in India's space sector under the Indian Space Policy 2023 and the Norms, Guidelines and Procedures issued by IN-SPACe.

Alongside his technology law practice, Goswami maintains an active corporate and commercial litigation practice. His litigation experience spans sectors with very different legal cultures and regulatory environments - the practical consequence is an advisory practice grounded in adversarial reality rather than theoretical preference. Clients who have worked with Goswami note that his advice is characterised by an unusual directness about legal risk: what the law says, where it is genuinely uncertain, and what the consequences of a given course of action are likely to be.

Goswami writes on artificial intelligence, technology policy, blockchain law, and digital regulation. His writing is addressed to the same audience as his practice i.e. founders, operators, and executives who are making decisions in areas of law that are still being shaped, and who benefit from analysis that is honest about the limits of current legal certainty rather than falsely reassuring about it.

He is recognised as one of the top voice in the tech legal community- an identity that reflects both the origin of his public engagement with technology law and the evolution of his practice from a Web3 focus to a broader technology law remit encompassing AI, space, and digital regulation.

APPROACH TO PRACTICE

The best legal counsel does not merely identify risk. It provides the clarity that allows clients to decide what to do about it.

Goswami's approach to client work is shaped by two convictions developed over more than a decade of practice.

The first is that legal advice in technology sectors must be grounded in genuine technical understanding — not to the level of an engineer, but to the level necessary to understand what a client is actually building, what regulatory classifications are genuinely applicable to it, and what legal risks are real rather than theoretical. Advice that does not understand the technology it is advising on is advice that does not understand the risk.

The second is that the most valuable legal counsel is counsel delivered before a problem arises, not after. The legal crises that most damage technology companies such as IP ownership disputes surfacing in due diligence, regulatory inquiries into businesses that assumed regulatory silence meant regulatory permission, contract disputes arising from specifications that were never precise enough to be enforceable — are almost always foreseeable from the outset.

The work of a good technology lawyer is to make them visible, and addressable, before they become crises.

SELECTED AREAS OF EXPERIENCE

AI & emerging technology

-AI contract structuring for SaaS and enterprise deployments, including IP ownership, training data restrictions, and liability allocation.

-Advisory on AI product compliance under the DPDP Act, 2023 and EU AI Act for companies with international operations.

-Legal analysis of AI system liability in regulated sectors including financial services and healthcare

-Advisory on the legal status of AI-generated content under different IP regimes.

Space law

-Advisory on IN-SPACe authorisation processes under ISP 2023 and NGP 2024 for private space operators.

-Remote sensing data commercialisation advisory under RSDP 2011.

-Insurance structuring for launch and in-orbit activities.

-Analysis of India's obligations under international space treaties and their implications for private operators

Crypto & Web3

-FIU-IND registration and PMLA compliance programme design for virtual asset service providers.
-Token structuring and regulatory classification analysis for issuers in India and offshore.
-DAO legal structuring through Indian and offshore entity frameworks.
-Smart contract legal documentation and parallel agreement drafting.
-Representation in regulatory inquiries involving crypto exchange operations.
- Hack response & recovery.

Litigation & arbitration

-Commercial dispute management across technology, FMCG, petroleum, and financial services sectors.
-Domestic and international arbitration, including institutional proceedings under SIAC and domestic rules.
-Regulatory enforcement response and representation in inquiries before MeitY, SEBI, RBI, and FIU-IND.
-Crisis management and first-response advisory in acute legal situations

SELECTED PUBLICATIONS & MEDIA

Goswami has contributed to The Hindu, The Telegraph, and Mint on blockchain regulation, technology policy, and digital law. His writing addresses the practical legal questions most relevant to India's technology sector i.e. regulatory compliance, contractual risk, and the legal implications of technological change at a level of specificity and accuracy that distinguishes it from general commentary.

He has published the AT & Partners Tech Law Guide for Startups, an annual practitioner's reference covering AI law, cryptocurrency regulation, Web3, space law, technology contracts, and corporate litigation available at www.atandpartners.in.

Media and conference enquiries may be directed to office@atandpartners.in.

FOREWORD

India is building across artificial intelligence, blockchain, Web3, space technology and digital platforms. Indian founders and companies are working at a pace that consistently outstrips the development of the legal frameworks designed to govern them. In most jurisdictions, the law follows technology by a decade or more. In India, that gap is both a challenge and an opportunity.

This guide is written for the people in that gap i.e. founders, operators, in-house counsel, and business leaders who are building at the intersection of technology and law, often without a clear map of the terrain.

It is not a comprehensive legal treatise but a practitioner's guide written from over a decade of advising companies through technology transactions, regulatory challenges, litigation, and the quiet legal crises that most founders encounter too late. Each section covers what I have found founders most need to understand, and most frequently misunderstand.

The areas covered are AI, crypto and blockchain regulation, Web3, space law, technology contracts and corporate litigation. These areas are not independent of each other but rather reflect a convergence of multiple disciplines working together.

Though the guide is structured by area but the principles that run through it are consistent i.e. understand the framework before you build, get your contracts right before you raise, and never assume that regulatory silence means regulatory permission.

I have tried being clear, direct, and useful without being reductive so where the law is genuinely uncertain, I have said so, where founders consistently make the same mistakes, I have said that too.

I hope as readers, you find it useful.

CHANDAN GOSWAMI

HOW TO USE THIS GUIDE

Each chapter in this guide is structured in two layers. The first layer explains the legal framework i.e. what the law says, what the regulatory position is, and where the genuine uncertainty lies.

The second layer is the practical layer i.e. what this means for your business, what to do, what to check, and what mistakes to avoid.

Three types of boxes appear throughout:

Legal note

Explains the legal framework, a significant case, or a regulatory position you need to understand.

Practical tip

Tells you what to actually do. Concrete, actionable, based on what works in practice (not what the textbook says).

Red flag

Identifies the mistakes that most commonly surface in due diligence, disputes, and regulatory inquiries. If you see this, stop and check.

CHAPTER 1: ARTIFICIAL INTELLIGENCE

Artificial intelligence is the defining legal frontier of this decade. The regulatory frameworks are still being written in India, in Brussels, and in Washington. However, legal exposure for companies building and deploying AI systems is already being litigated in some jurisdictions.

What this means is that the associates risks are no longer theoretical and the Courts are being asked to answer questions that legislation has not yet fully settled.

1.1. WHO OWNS WHAT AN AI SYSTEM CREATES?

(a) Intellectual property ownership in AI-generated outputs is one of the most contested questions in technology law today. Under current Indian law, copyright subsists in works created by human authors and since the Copyright Act, 1957 does not contemplate non-human authorship it gives rise to the question of whether AI-generated content (text, images, code, music) can be owned? And if yes, then by whom. This has no settled answer in India.

(b) For all practical purposes, founders should ensure that their AI contracts, whether with model providers or with clients, explicitly address IP ownership because a contract that is silent on this point creates ambiguity that will surface at the worst possible moment (during a fundraise, an acquisition, or a dispute).

(c) Therefore, ensure that your terms of service, client contracts, and employment agreements each explicitly address ownership of AI-generated outputs. Do not assume that the default IP provisions in your standard agreements cover this.

Practical tip: what to actually put in your AI IP clause

Your AI-related contracts, whether with model providers, with clients, or in your employment agreements should explicitly address three questions: (1) who owns outputs generated using the AI system; (2) whether your input data is used by the vendor to train or improve their models; and (3) what happens to derivative works or outputs that are modified or incorporated into a larger product.

A workable clause may read as follows: *'All outputs generated by the AI system using Client data or inputs shall be the exclusive property of Client. Vendor shall have no right to use Client data or Client-generated outputs for model training, improvement, or any purpose other than service delivery without Client's prior written consent.'*

Note that this is not a standard clause in AI agreements. You will need to negotiate it.

Red flag : check your OpenAI, Google, and AWS terms

The default terms of the major AI API providers such as OpenAI, Google (Gemini), Anthropic, AWS (Bedrock) vary significantly on data usage and IP ownership. Some reserve the right to use your inputs for model improvement unless you opt out. If you are building a product on top of these APIs and your clients' data flows through them, your downstream client contracts may conflict with your upstream vendor terms. Check both before you commit.

1.2. AI LIABILITY : WHEN THE MODEL GETS IT WRONG

(a) As AI systems are deployed in higher-stakes environments such as medical diagnosis, financial advice, legal research, and autonomous vehicles, the question of liability for AI errors becomes more pressing. Though the current Indian consumer, and contract laws may apply but neither was designed with AI systems in mind.

(b) The key questions which arise for consideration are- who bears liability when an AI system causes harm? The model developer, the deploying company, the user, or a combination? In my understanding, in most cases the answer will depend on the contractual framework, the nature of the deployment, and whether the harm was foreseeable.

(c) Founders deploying AI in regulated sectors (healthcare, financial services, insurance etc.) should be particularly careful. Regulatory regimes in these sectors impose obligations that interact with AI deployment in ways that are not always obvious. At a baseline, the Digital Personal Data Protection Act, 2023 may apply wherever personal data is used for training, fine-tuning, or decision-making.

(d) In the realm of financial services, entities regulated by the Reserve Bank of India, Securities and Exchange Board of India, and Insurance Regulatory and Development Authority of India must align AI use with existing outsourcing, risk management, and IT governance norms.

(e) AI systems that influence diagnosis or treatment may fall within the scope of the Drugs and Cosmetics Act, 1940 and be regulated as software as a medical device (SaMD). What it actually means is that AI does not sit in a regulatory vacuum but plugs into existing obligations.

Practical tip: how to structure AI liability in your client contracts

If you are deploying an AI product to clients, your agreement should do four things: first, disclaim liability for AI errors that result from inaccurate or incomplete inputs provided by the client. Second, cap your liability for AI-related errors at a figure that reflects your insurance coverage and commercial reality. Third, require the client to maintain human oversight for any decision

with material consequences. Fourth, require the client to notify you promptly of any AI errors allowing you to fix problems before they compound.

A liability cap tied to twelve months of fees paid is standard, but may be inadequate for high-stakes deployments.

Practical tip: how to manage regulatory uncertainty

In the absence of comprehensive AI regulation, the practical approach is to document your decisions. When you make a design or deployment choice that has a regulatory dimension i.e. deciding not to include a human review step, deciding to use personal data for model training, or deciding that your AI output does not constitute regulated advice write down the reasoning at the time. This contemporaneous record is your primary defence in any future regulatory inquiry.

The companies that are most exposed to emerging regulation are not those with genuinely problematic products but are those with reasonable products and no documentation of why their choices were reasonable.

Sector-specific note

Founders deploying AI in healthcare, financial services, or insurance face an additional layer of risk. Regulatory regimes in these sectors impose obligations on accuracy, on auditability, and on explainability. A general tech liability clause may not cover a misdiagnosis or an erroneous credit refusal.

1.3 THE EU AI ACT AND INDIAN COMPANIES

(a) The EU AI Act applies to any AI system that is placed on the EU market or whose outputs are used within the EU, regardless of where the developer is base which implies that an Indian startup with even a small number of European users may fall within its scope.

(b) The Act creates a tiered risk framework. High-risk AI applications including those used in recruitment, credit scoring, critical infrastructure, and law enforcement are subject to the most stringent requirements. AI systems that manipulate behavior through subliminal techniques and those that enable social scoring by public authorities come under the ambit of prohibited applications.

(c) So, if your product has any EU-facing users or partners, conduct an EU AI Act scoping exercise before your next product launch. The compliance obligations for high-risk applications are significant, and the penalties for non-compliance are material.

Practical tip: a five-step EU AI Act scoping exercise

Step 1: List every jurisdiction in which your AI product is used or accessible. If any are any EU member states, proceed to Step 2.

Step 2: Classify your AI application against the Act's risk tiers. Most B2B SaaS AI products fall in the 'limited risk' or 'minimal risk' tier. However, do not assume. Recruitment tools, credit scoring tools, and content recommendation systems may qualify as high-risk.

Step 3: If you are high-risk, identify the mandatory requirements: conformity assessment, technical documentation, human oversight mechanisms, accuracy and robustness standards, registration in the EU database.

Step 4: Review your data practices against the Act's training data transparency requirements, particularly if you are building a GPAI model.

Step 5: Appoint a compliance expert for EU AI Act compliance before you launch in any of the EU markets. The fines - up to 3% of global annual turnover for certain violations - are not nominal.

Red flag: 'AI' in your marketing without substance in your product

Sector regulators are increasingly alert to 'AI washing' products marketed as AI-powered but are not. If your marketing materials make AI capability claims, ensure your product actually delivers them and that you can substantiate them with technical documentation.

CHAPTER 2: CRYPTOCURRENCY, WEB3 AND BLOCKCHAIN

India's regulatory approach to cryptocurrency has been among the most closely watched and most frequently changed in the world. After years of uncertainty, including a brief period of prohibition, the current position is that cryptocurrency trading and holding is legal, but heavily taxed.

While we wait for the framework to evolve, the companies operating in this space must keep themselves abreast with regulatory changes rather than relying on advice that may have been received a year ago.

Web3 encompasses a broad range of technologies and business models. Decentralised applications, NFT platforms, DeFi protocols, metaverse infrastructure, are some examples.The legal treatment of each varies, and the area is evolving rapidly. This chapter addresses the most practically relevant questions for founders building in this space.

2.1. THE CURRENT REGULATORY FRAMEWORK IN INDIA

(a) Virtual Digital Assets (VDAs), as defined under the Income Tax Act, 1961 (as amended in 2022), are subject to a flat 30% tax on gains, with no deduction permitted except the cost of acquisition. A 1% TDS applies to transfers above specified thresholds. Needless to say, these provisions have significantly affected trading volumes and business models in the Indian crypto ecosystem.

(b) Additionally, entities providing crypto exchange services, wallet services, and related financial services are now subject to the Prevention of Money Laundering Act (PMLA) framework, following the March 2023 notification by the Ministry of Finance. Compliance obligations include customer due diligence (KYC), suspicious transaction reporting, and record-keeping requirements that mirror those applicable to traditional financial institutions.

Practical tip: FIU-IND registration, step by step process.

If you operate a Virtual Asset Service Provider (VASP) [exchange, wallet, custodian, transfer service] you are required to register with the Financial Intelligence Unit India (FIU-IND). Here is what the process actually involves-

1. Registration is done through the FIU-IND reporting entity portal (fiuindia.gov.in). You will need your entity's PAN, GST registration, details of the Principal Officer and Designated Director, a documented AML/CFT policy, and evidence of KYC procedures.

2. The most common reason for delays is inadequate AML/CFT documentation. Your policy must address customer due diligence, enhanced due diligence for high-risk customers, transaction monitoring, suspicious transaction reporting (STR), and record retention for a minimum of five years.

3. Budget approximately four to six weeks for the process if your documentation is in order from the start. Pro tip is to engage a compliance officer before you file, not after.

Red flag : operating without FIU-IND registration

The enforcement position on unregistered VASPs has hardened significantly since 2023. Several international exchanges were blocked for non-compliance. Operating as a VASP without FIU-IND registration exposes the entity and its directors personally to prosecution under PMLA. There is no grace period and no 'good faith' defence for straightforward non-registration.

2.2. TOKEN STRUCTURING AND CLASSIFICATION

The classification of a token as a security, a utility, a commodity, or a payment instrument determines which regulatory framework applies. An instrument structured as a utility token but functioning as an investment vehicle is likely to attract scrutiny under securities law.

Practical tip : a working token classification framework

Before structuring any token, work through these four questions with legal counsel.

First: does the token represent an investment of money in a common enterprise with an expectation of profit from the efforts of others? If yes, it is likely a security under the Howey-equivalent analysis in the jurisdiction it is engaged in.

Second: does the token have a primary utility such as access to a platform, a service, or a product that is operational at the time of sale? A utility token sold before the utility is available looks like a security in practice, whatever it is called in documentation.

Third: is the token freely transferable on secondary markets? Transferability increases the likelihood of securities characterization.

Fourth: does your marketing material emphasize potential returns or appreciation? If yes, you are marketing a security regardless of the token's technical structure.

Document this analysis in a legal opinion obtained before launch. If the analysis is genuinely borderline, engage with regulatory framework experts before proceeding.

2.3. EXCHANGE COMPLIANCE AND OPERATIONAL REQUIREMENTS

Crypto exchanges operating in India must maintain a compliant AML/KYC programme not merely a registration and the distinction matters. Registration is a one-time act but compliance is an ongoing operational requirement.

Practical tip: building a minimum viable compliance programme

A compliant operation requires five components that must be operational, not just documented.

1. Customer identification and verification (KYC): Collect and verify government-issued ID and PAN for all customers. For high-value customers, collect source of funds documentation.

2. Transaction monitoring: Implement automated monitoring for patterns associated with money laundering i.e. structuring (multiple transactions just below reporting thresholds), rapid cycling, transactions to high-risk jurisdictions. Off-the-shelf blockchain analytics tools (Chainalysis, Elliptic, TRM Labs) cover the on-chain component.

3. Suspicious transaction reporting (STR): File STRs with FIU-IND within seven working days of identifying a suspicious transaction. Maintain a log of all STR decisions, including decisions not to file.

4. Maintain KYC and transaction records for a minimum of five years after the relationship ends.

5. All customer-facing and compliance staff must receive documented AML training, at least annually.

2.4. DAO LEGAL STRUCTURES IN INDIA

DAOs occupy an uncertain legal position in India. There are no DAO-specific legislations and no recognised DAO entity type. A DAO operating in India or whose members are based in India would have to be structured through an existing entity type.

Which structure could work-

The structure depends on what the DAO does. Here is the practical matrix-

1. If the DAO is primarily an investment vehicle i.e. pooling funds to invest in DeFi, NFTs, or other assets, it resembles an Alternative Investment Fund and SEBI's AIF regulations may apply. The safest structure for an India-based investment DAO may be an offshore entity (Cayman Islands or Singapore) with Indian members participating through FEMA-compliant investment routes.

2. If the DAO operates a protocol or platform such as a DeFi protocol, a marketplace, or a game, the operational entity could typically be a Singapore private limited company or a Cayman foundation, with a separate India entity for team employment and local operations.

3. If the DAO is primarily a community or contributor collective with no significant financial flows a simpler structure such as an LLP or Section 8 company may work domestically.

In all cases the DAO's governance documentation (its constitution, voting rules, and member rights) should have a parallel legal document that is enforceable in a real court. Smart contracts alone are not a substitute.

2.5. SMART CONTRACTS : LEGAL ENFORCEABILITY IN PRACTICE

(a) As a matter of law, a contract is valid and enforceable agreement if offer, acceptance, consideration, and the intention to create legal relations are present. A smart contract on the other hand is just a computer programme that executes automatically when certain predefined conditions are met.

(b) A smart contract governs a commercial relationship without any governing law clause, dispute resolution mechanism, or human-readable documentation of intent which makes it a source of legal risk.

(c) This gives rise to certain practical complications that smart contracts are not equipped to handle or may perhaps handle poorly. For instance, change in circumstances, disputes about intent, and the need to interact with off-chain legal systems are beyond the scope of a smart contract.

(d) Since smart contracts are essentially a computer programme, they do not come under the direct ambit of contract law unless they are supplemented with an additional written contract.

Practical tip : the parallel documentation approach

The most robust approach combines on-chain smart contract execution with traditional off-chain legal documentation. The smart contract handles performance while the legal agreement handles everything the smart contract cannot such as governing law, dispute resolution, intent, force majeure, and remedies for smart contract bugs.

The two documents should cross-reference each other i.e. the legal agreement may state: *'The smart contract deployed at*&^%$s45527B on SUPERchain constitutes the automated performance mechanism for this agreement. In the event of conflict between this agreement and the smart contract code, this agreement governs.'*

This approach adds perhaps two to three days of legal drafting time and avoids the far more significant time and cost of a dispute about what the parties intended.

Red flag : unaudited smart contracts governing material financial flows

If your smart contract governs material financial flows such as user funds, protocol treasury, token distributions, and it has not been audited by a reputable code auditor, you may face two distinct problems. First, the technical risk of a bug or exploit (which is a business risk, not strictly a legal one). Second, the legal risk that a bug causing user losses will be characterised as negligence, and that the absence of an audit will be evidence of that negligence. Smart contract audits are commercially available from firms such as Certik, Trail of Bits, and ConsenSys Diligence etc. For any contract holding more than a nominal amount, an audit is not optional.

CHAPTER 3: SPACE LAW AND THE NEW SPACE ECOSYSTEM

India's space sector has opened significantly to private participation, but the legal framework governing it is still maturing. A critical starting point here is that India though India currently has no comprehensive domestic legislation governing space activities, the sector is still governed by the Indian Space Policy, 2023 and the Norms, Guidelines and Procedures for Implementation of Indian Space Policy 2023 (NGP 2024) issued by IN-SPACe. A dedicated Space Activities Bill is under active consideration by the government but has not yet been enacted.

3.1. THE AUTHORISATION FRAMEWORK

(a) Indian National Space Promotion and Authorisation Centre (IN-SPACe) functions as the single-window authorisation body for non-government private space activities in India under the NGP 2024. Any Indian private entity wishing to undertake space activities including satellite manufacturing, launch services, ground station operation, and downstream data services requires IN-SPACe authorisation.

(b) India is a contracting party to the major UN space treaties such as the Outer Space Treaty 1967, the Rescue Agreement 1968, the Liability Convention 1972, and the Registration Convention 1975. Though India is a signatory to the Moon Treaty 1979 but has not ratified it. A signatory state has a distinct legal status, it is bound by the obligation not to act contrary to the object and purpose of the treaty, even without the full obligations of ratification.

(c) These treaties impose obligations on the Government of India and through the corresponding obligations flow down to private operators authorised by IN-SPACe.

Practical tip: how to navigate the IN-SPACe authorisation process

The IN-SPACe process has three stages: an Expression of Interest (EoI), a technical review, and a formal authorisation. Here is what the process looks like in practice-

The EoI stage is the most important for early-stage companies. IN-SPACe uses the EoI to assess the seriousness of the applicant and the viability of the proposed activity. A well-prepared EoI covering the technical concept, the commercial model, the team's credentials, and the timeline creates a working relationship with IN-SPACe that is valuable throughout the authorisation process. A poorly prepared EoI creates an impression that is difficult to reverse.

We recommend engaging a legal counsel before submitting the EoI and not after. The framing of your activity i.e. how you describe what you are doing, determines the regulatory requirements. An activity described as a 'satellite communications service' faces different requirements from one described as a 'remote sensing data analytics service.'

The authorisation timeline, from EoI to formal authorisation, currently runs at approximately nine to eighteen months for straightforward applications.

Red flag: assuming ISRO partnership equals authorisation

Several early-stage space startups have proceeded under the assumption that a commercial arrangement with ISRO or ANTRIX substitutes for IN-SPACe authorisation. IN-SPACe authorisation is a separate, mandatory regulatory requirement for all private space activities, regardless of whether an ISRO partnership exists.

3.2. DATA AND REMOTE SENSING

Satellite-derived remote sensing data is governed by the Remote Sensing Data Policy 2011 (RSDP 2011), issued by the Department of Space on July 4, 2011. This is the operative policy for any company seeking to acquire, commercialise, or distribute satellite imagery in India. It applies to data from both Indian and foreign satellites. The National Remote Sensing Centre (NRSC), under ISRO and DOS, is vested with the authority to acquire and disseminate all satellite remote sensing data in India.

Practical tip : data commercialisation without regulatory exposure

The practical framework for commercialising remote sensing data in India requires three clearances to be in place before you launch a commercial data product.

First, IN-SPACe authorisation covering the data collection activity and not just the satellite operation.

Second, compliance with the Remote Sensing Data Policy (RSDP), which restricts the resolution and content of imagery that can be shared with foreign parties. The current policy permits sharing of imagery with ground resolution above one metre with most foreign parties, but sub-metre imagery is subject to case-by-case government approval.

Third, for data involving national security-relevant areas defence installations, border regions, critical infrastructure a security clearance process applies regardless of resolution.

Map your product's data specifications against these requirements before you sign commercial contracts with international customers. Promising delivery of data that you cannot legally provide is a contractual liability.

CHAPTER 4: TECHNOLOGY CONTRACTS

Technology contracts are the legal infrastructure on which companies are built. This is also an area where make avoidable mistakes are made; not because of lack of diligence but because standard contract templates do not address the specific legal terrain of technology companies. It is amusing to note that the consequences of such contract failures typically materialise at the worst possible moment.

4.1. THE CLAUSES THAT MATTER

These provisions consistently require specific attention in technology services agreements and are most frequently drafted inadequately.

a. Data ownership on termination: Who owns the data? What format will it be returned in? Within what timeframe? A vendor who *'owns'* your data or who returns it in a proprietary format that you cannot use has effective leverage over your business that does not appear on any risk register until it is too late.

b. IP in customisations: If you request custom development, who owns the resulting IP? The default position in most vendor agreements is that the vendor owns all modifications and improvements. This is negotiable, and it matters significantly if the customisation is core to your product.

c. Liability cap: The standard mutual cap at twelve months of fees paid may be appropriate for a commodity SaaS subscription. It is likely inadequate if you are using the software for mission-critical operations. Know what you are agreeing to and ensure your cap is at least commensurate with the potential loss.

d. SLA remedies: Service level agreements in standard form typically offer *service credits/discounts on future invoices* as the remedy for downtime. Service credits are worth nothing to a business that has suffered material harm from an outage. Negotiate for the right to terminate and recover direct losses for material, sustained SLA failures.

e. Audit rights: If the vendor processes your data or your clients' data, you need the contractual right to audit their security practices. 'We are ISO 27001 certified' is not an audit right. A certification can be stale but right to audit is live.

Red flag : auto-renewal clauses with short cancellation windows

The most common contractual trap in SaaS agreements is the auto-renewal clause combined with a short cancellation notice window i.e. typically 30 to 60 days before the renewal date. Companies routinely miss these windows and find themselves locked into another annual contract with a vendor they intend to leave. Diarize renewal dates and cancellation deadlines at the time of signing and not when the invoice arrives.

4.2. AI-SPECIFIC CONTRACT PROVISIONS

Contracts governing AI products and services require provisions that do not appear in standard technology agreements. The following are the minimum AI-specific terms that should appear in any agreement where AI output is a material component of the service.

Practical tip : the AI contract clause checklist

Include these six provisions in any AI-related commercial agreement, whether as a vendor or as a customer.

1. Output ownership: Explicitly state who owns AI-generated outputs. Do not leave this to implication.

2. Training data prohibition: If you do not want your data used to train the vendor's models, say so explicitly: *'Vendor shall not use Client data, Client inputs, or Client-generated outputs to train, fine-tune, improve, or evaluate any AI model without Client's prior written consent.'*

3. Accuracy disclaimer and human oversight requirement: The agreement should acknowledge that AI outputs may be inaccurate and require that material decisions based on AI outputs be subject to human review. This is both a legal protection and, increasingly, a regulatory requirement.

4. Model change notification: AI vendors update their models regularly. A model update can change the performance, behaviour, and accuracy of the service you contracted for. Include a requirement for advance notice of material model changes and a right to test before the change goes live.

5. Hallucination liability: Address liability explicitly for cases where the AI generates factually incorrect outputs, particularly in sectors where accuracy is critical (legal, medical, financial). The allocation should reflect the actual risk distribution between the parties.

6. Data security specific to AI inputs: AI systems that process sensitive personal data or confidential business information require security commitments that go beyond standard data security clauses including controls on who at the vendor organisation can access your data and whether it flows through third-party infrastructure.

5.3. EMPLOYMENT AND FOUNDER AGREEMENTS

Intellectual property assignment provisions in employment and founder agreements are among the most consequential documents a startup will sign, and among the most frequently ignored. The consequences of ignorance surface at a much late stage where they are harder and more expensive to fix than if they had been addressed at the outset.

Practical tip : the IP assignment audit every startup should run

Run this audit before your next fundraise, and again before any M&A process.

First: identify every person who has contributed to any material IP in your product or business. Be it a code, design, content, algorithms, or processes. Include founders, employees, contractors, freelancers, and advisors.

Second: for each person, identify whether a signed IP assignment agreement exists that covers the relevant work. 'They worked for us' is not IP assignment. 'They signed a standard employment agreement' may not be IP assignment, depending on what the agreement says and when the work was created.

Third: for any pre-incorporation work created by founders before the company existed identify whether that work has been formally assigned to the company by a documented instrument.

Fourth: for any contractor or freelancer work, identify whether the contract includes a work-for-hire provision and an IP assignment. The default position for contractors is that they retain IP unless specified. This surprises many founders.

Fifth: for any open-source components used in your product, identify the licence and check whether it is compatible with your commercial use. Further, ensure you are complying with the licence terms particularly around attribution and derivative work restrictions.

4.4. DPDP ACT COMPLIANCE IN CONTRACTS

The Digital Personal Data Protection Act, 2023 imposes obligations on data fiduciaries and creates corresponding obligations in contracts with data processors. Most standard vendor agreements predating the Act do not contain the required provisions.

Practical tip : the DPDP contract update checklist

Review every agreement under which a third party processes personal data on your behalf. Cloud providers, analytics vendors, HR software, payment processors, marketing platforms all fall under this. Ensure the following provisions are in place-

One: a data processing agreement (DPA) or equivalent addendum that specifies the processing purpose, the categories of data, the retention period, and the security obligations.

Two: a sub-processor clause that requires the processor to obtain your approval before engaging a sub-processor and to flow down equivalent obligations.

Three: a data breach notification clause requiring the processor to notify you within 72 hours of becoming aware of a breach which is the timeframe you need to meet your own notification obligations under the Act.

Four: a deletion or return obligation at contract termination wherein the processor must delete or return all personal data, and confirm in writing that deletion has occurred.

Five: an audit right to verify the processor's compliance with the obligations.

CHAPTER 5: CORPORATE AND TECHNOLOGY LITIGATION

Litigation is the part of legal practice that most founders hope they will never need. The companies that are best positioned when litigation arises are those that have treated legal risk management as an operational matter rather than an emergency response. This chapter covers both preparation and response.

5.1. THE FIRST 48 HOURS OF A DISPUTE

What a company does and fails to do in the first 48 hours after a dispute crystallises has a disproportionate impact on the outcome. Most of the avoidable errors in litigation arise from actions taken before lawyers are properly instructed.

Practical tip : your first 48-hour dispute response protocol

The moment you receive a legal notice, a serious complaint, or become aware of a potential dispute, do the following.

1. Do not respond without legal advice: Even a casual email acknowledging receipt can be used against you. If you really must acknowledge receipt, say 'We acknowledge receipt of your letter and are seeking legal advice. We will revert within x number of days.'

2. Issue a document preservation notice internally: Send a written instruction to all relevant employees requiring them to preserve and not delete, modify, or move all documents, emails, messages, and data that may be relevant to the matter. Courts draw adverse inferences from document destruction that occurs after a dispute is foreseeable.

3. Inform your lawyers immediately: The first instinct of many founders is to attempt to resolve the matter commercially before engaging lawyers. This is sometimes correct, but the commercial conversation should happen with full awareness of the legal position for which lawyers need to be involved first.

4. Do not discuss the matter on unprotected channels: Communications between a client and their lawyer are privileged. Communications between founders or employees about the matter are not and they are discoverable.

Red flag : WhatsApp as a legal liability

In almost every dispute we have managed, WhatsApp messages between founders, employees, or counterparties have been significant evidence. People say things in WhatsApp that they would never put in email. Once a dispute is foreseeable, treat every internal communication as if it will be read in open court before a judge. This is not paranoia but a practice in reality.

5.2. COMMON TECHNOLOGY SECTOR DISPUTE PATTERNS

Certain dispute patterns recur with notable consistency in technology sector litigation. Awareness of these patterns allows companies to structure their commercial relationships to reduce exposure.

Practical tip: the contract specification problem and how to avoid it

The most common technology dispute arises from inadequately specified deliverables. The solution is a specification document that is specific enough to be independently verifiable. For each deliverable, specify what it does (functional requirement), how well it does it (performance requirement), how you will know it has been achieved (acceptance test), and what happens if it is not achieved by the agreed date (consequences of delay).

The acceptance test is the most important element and one of most frequently omitted. 'The system shall be delivered to the client's satisfaction' is not an acceptance test. *'The system shall process 10,000 transactions per second with a 99.5% success rate, as measured by [a specified test] conducted by [a specified party] within [a specified timeframe] of delivery'* is an acceptance test.

A well-drafted specification document adds time at the front of a project. Not only does it save multiples of that time but also significant legal cost by eliminating the most common source of technology disputes.

5.3. ARBITRATION : CHOOSING THE RIGHT MECHANISM

For technology companies with international counterparties, arbitration is generally preferable to court litigation. The arbitration clause should be a considered decision, not a boilerplate afterthought.

Practical tip : how to draft an arbitration clause that works

An arbitration clause has six components, each of which should be a deliberate choice.

1. The institution: For domestic commercial disputes, DIAC (Delhi International Arbitration Centre) or MCIA (Mumbai Centre for International Arbitration) are practical choices. For cross border/ international disputes, SIAC (Singapore) provides excellent enforceability of awards across Asia. ICC is appropriate for large, complex disputes with European counterparties.

2. The seat: The seat determines the procedural law of the arbitration and the courts that have supervisory jurisdiction. Singapore is the most common seat for international tech disputes. London, Dubai (DIFC), and Mumbai are also used. Choose based on your counterparty's preference and your assessment of the relevant courts.

3. The governing law of the contract: This is separate from the seat. Your contract can be governed by Indian law and seated in Singapore.

4. The number of arbitrators: A sole arbitrator is faster and cheaper. However, a three-member Tribunal is more thorough. For disputes below 2 crore INR, a sole arbitrator is generally

appropriate. Nevertheless, the parties can choose the number depending upon their commercial appetite.

5. The language: State it explicitly, especially in cross-border agreements.

6. Emergency relief: Consider whether to include access to emergency arbitrator provisions for situations requiring urgent interim relief before a Tribunal is constituted.

A well-drafted arbitration clause takes approximately 30 minutes to agree. A poorly drafted clause or the absence of one can add months and significant cost to any dispute.

5.4. REGULATORY ENFORCEMENT: PREPARATION IS EVERYTHING

As AI, crypto, and technology regulations mature, regulatory enforcement will become an increasingly significant component of legal risk. Companies that are prepared for regulatory engagement are in a fundamentally different position from those that are not.

Practical tip : building a regulatory readiness file

A regulatory readiness file is a set of documents that you maintain on an ongoing basis and that allow you to respond efficiently and effectively to any regulatory inquiry. It should contain the following-

One: a description of your business and its regulatory classification in your own documented analysis of which regulations apply to your activities and why.

Two: a compliance history containing all records of regulatory filings, registrations, licences, and correspondence with regulatory authorities.

Three: a legal opinion or advice memo on any material regulatory question you have faced, and the decision made post receiving the opinion or memo.

Four: documentation of your key policies such as data protection, AML/KYC, AI governance, security with their documented history showing when they were adopted and updated.

Five: a record of any previous regulatory inquiries and how they were resolved.

This file is not primarily useful for regulatory inspections but comes in handy when you have to be conscious of your regulatory position on an ongoing basis. This, in our view, may be the most effective form of regulatory risk management.

CONCLUSION: BUILDING IN THE GAP

Every area of law covered in this guide shares a common condition: the legal framework is incomplete, the regulatory position is still evolving, and the consequences of navigating it poorly fall directly on the companies and individuals who are building within it. That is not a temporary state of affairs. It is the permanent condition of technology law, because technology will always move faster than the institutions designed to govern it.

What changes over time is not the existence of the gap, but its location. A decade ago, the gap was in basic internet commerce and data law. Five years ago, it was in blockchain and cryptocurrency. Today it is most acute in artificial intelligence, space technology, and the intersection of all of these with India's emerging data protection framework. In five years, it will be somewhere else and the companies that are best positioned then will be the ones that learned, in this period, how to operate thoughtfully in legal uncertainty rather than waiting for certainty before proceeding.

"Legal uncertainty is not a reason to stop building. It is a reason to build with greater awareness of where the risks lie."

The consistent lesson from over a decade of advising companies through these areas is not that the law is hostile to technology, or that regulation inevitably lags behind innovation in ways that cannot be managed. The lesson is more specific: the legal problems that damage technology companies most severely are almost always foreseeable, and almost always addressable before they become crises.

The AI contract that did not address IP ownership. The crypto compliance programme that was documented but never operational. The technology agreement with an acceptance test that was never specific enough to be applied. The WhatsApp thread that became the central exhibit in a dispute. None of these outcomes was inevitable. Each of them was the consequence of a decision made or deferred at a point when better information and earlier engagement with a lawyer would have produced a different result.

This guide is an attempt to move that engagement earlier and not to replace legal counsel ; no general guide can do that, and the specific questions that arise in any technology transaction or regulatory matter require advice that is calibrated to the specific facts. But to give the founders, operators, and in-house counsel who read it a more accurate map of the territory: what the law actually says, where it is genuinely uncertain, what the most common failure points are, and what the practical steps are to address them before they become problems.

Three principles have guided every section of this guide, and are worth stating plainly as a closing proposition.

RECAP

DOCUMENT YOUR DECISIONS

In areas of legal uncertainty which is most of technology law in India today the quality of your documentation is often the difference between a defensible position and an indefensible one. When you make a decision that has a regulatory dimension, write down the reasoning at the time. When you obtain legal advice on a novel question, keep the record of it.

When you decide not to file a suspicious transaction report, document why. When you determine that your AI product does not constitute regulated advice in a particular sector, record the analysis. This documentation is not bureaucracy. It is the contemporaneous record of a thoughtful, good-faith effort to comply with the law as it then stood and in any subsequent regulatory inquiry or litigation, it is your primary defence.

GET THE CONTRACTS RIGHT, AND GET THEM RIGHT EARLY

Technology companies are disproportionately dependent on their contracts because their most valuable assets- intellectual property, data, software, customer relationships - exist primarily as legal rights rather than physical objects. A technology company whose contracts do not clearly establish who owns its IP, what its liability exposure is, how its data is protected, and what happens when things go wrong is a company built on a foundation that has not been tested.

These things are always easier and cheaper to address before the contract is signed, before the product is launched, and before the dispute has arisen. The founding documents of a technology company - its founders' agreement, its employment agreements, its IP assignment instruments - deserve the same level of attention as its product, because they govern what the company actually owns.

ENGAGE WITH REGULATION, DO NOT WAIT FOR IT

The regulatory frameworks governing AI, cryptocurrency, Web3, and space technology in India are being built in real time. The companies that engage constructively with that process, responding to consultations, participating in working groups, raising practical concerns through proper channels, maintaining open relationships with regulators before problems arise are in a materially different position from those that treat regulation as something that happens to them. Regulatory engagement is not a substitute for legal compliance. But it is the most effective form of long-term legal risk management available to a technology company operating in a sector where the rules are still being written.

The areas of law covered in this guide will look different in two years. New statutes will have been enacted, new cases decided, new regulatory frameworks operationalised. This guide will be updated annually to reflect those changes. The underlying principles: document your decisions, get the contracts right, engage with regulation will not change, because they are not specific to any particular legal framework. They are the conditions of operating thoughtfully in a legal environment that is always, in some measure, incomplete.

If this guide has been useful, the most effective way to reciprocate is to raise the legal standard of the companies you build and advise. India's technology sector will be better for founders and operators who understand their legal environment not because it makes lawyers more necessary, but because it makes the companies stronger.

CHANDAN GOSWAMI