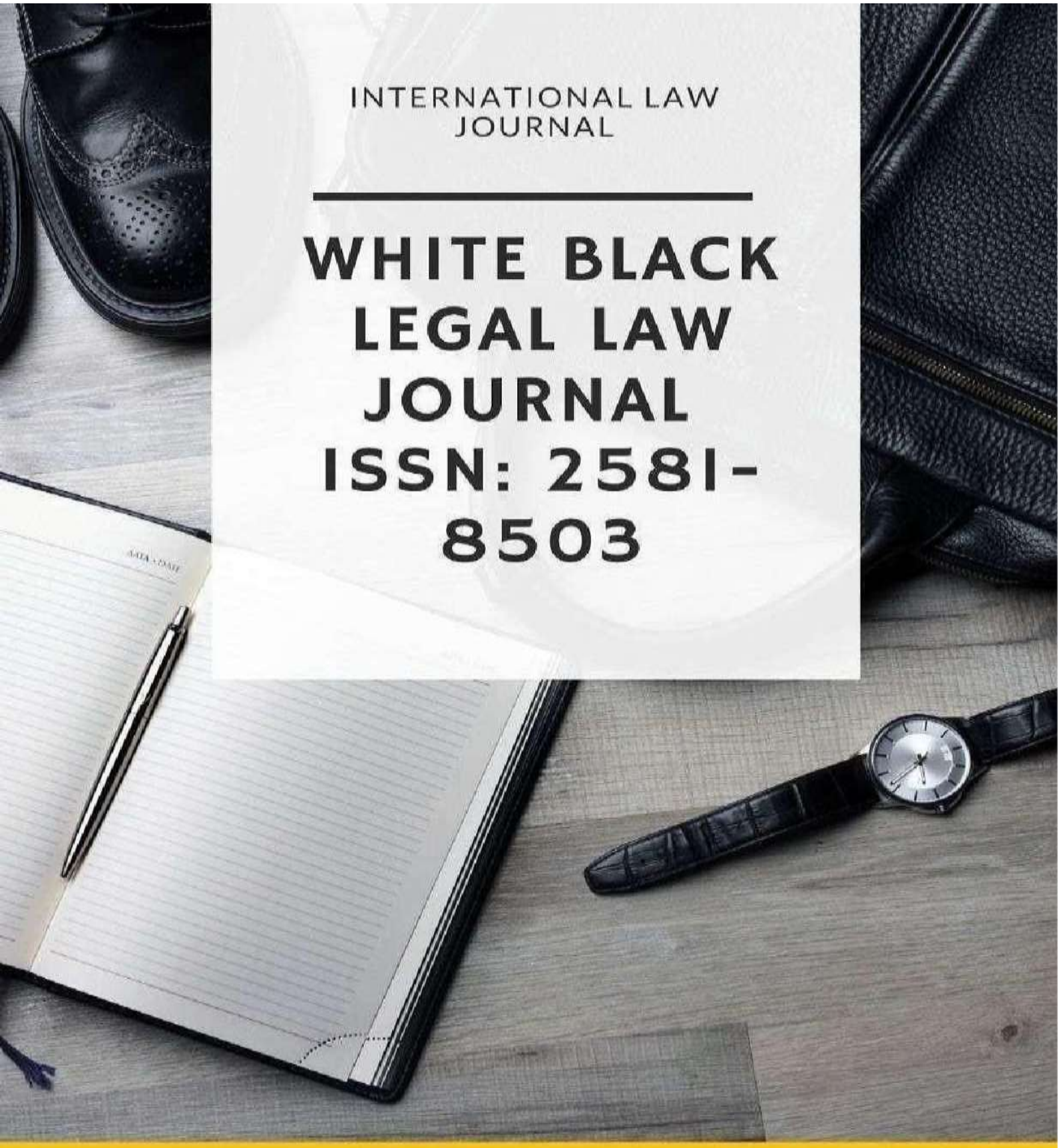

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

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

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

FUELING THE FUTURE: HOW VENTURE CAPITAL TACKLES REGULATORY UNCERTAINTIES IN DEEP-TECH AND AI STARTUPS

AUTHORED BY - SREEJEETA DAS & RITIKA SRIVASTAVA

Abstract

Venture Capital is a significant force in the progress of deep-tech and Artificial Intelligence (AI) startups since they face high regulatory complexities. The businesses proposed, which utilize innovations in the field of AI, machine learning, blockchain, and quantum computing, require huge investment and long-running research and development to solve urgent global problems. However, such stringent regulatory regimes, such as the European Union General Data Protection Regulation, and its future AI regulation, the Indian Digital Personal Protection Act and numerous state regulations in the U.S., have been erected, which limits access to markets and any scaling practices. The VCs overcome such risks by being thorough in due diligence, having superior intellectual property planning and partnership with legal experts, and ensuring ethical artificial intelligence practices and data management norms adherence. In screening innovation for regulatory compliance, VCs secure their investments as much as they expedite an impressive technology to become a global change game-changer.

Keywords: *Venture Capital, Deep-tech, Artificial Intelligence, Intellectual Property, AI Governance*

Introduction

Venture capitalists (VCs) are powerful financial intermediaries that do offer vital early-phase capital to prospective startup organizations, which generate commercialization and dispersion of innovations.[1] "Their investments in young firms are subject to high risks and uncertainties, and they are seminal in the making of the new technologies and business ideas to come to life."[2] Yet, the asymmetries that exist with the start of business, have created a more permanent dilemma since VCs are prone to making mistakes based on those information gaps. An

[1] Paul Gompers, Josh Lerner, *The Venture Capital Revolution*, 15 J. Econ. Perspect. 145–168 (2001).
[2] Nicolas Ameye, Jacques Bughin, N. van Zeebroeck, *How Uncertainty Shapes Herding in the Corporate Use of Artificial Intelligence Technology*. *Technovation, 127*, 102846 (2023).

illustrative chart is with regard to artificial intelligence (AI) that had been the subject of several hype and disappointment cycles apparently throughout the decades.[3] The new business models that deep tech startups are developing based on advanced technology include artificial intelligence (AI), machine learning, big data, augmented reality, and virtual reality, blockchain, robotics, cyber security, internet of things (IoT) and many more. Such high technological devices require massive funds to introduce to the market. "AI-related startups have maintained a technological uncertainty, market uncertainty, and regulatory ambiguity, although AI has recently seen significant breakthroughs in machine learning and neural networks, it is increasingly being adopted in the mainstream, catalyzed by such jump in technologies and recent breakthroughs in its sub-areas."[4]

"The opacity of AI seems to intensify the confusion facing VCs as they seek to figure out which novelties of startups could rightfully receive investment in the face of exaggeration. The growing importance of AI and simultaneously the existing ambiguities with regards to AI-related startups highlights the relevance to evaluate the mechanisms underpinning the ability of some of the VCs to better cope with the complexity of the AI landscape."[5] New firms find it a costly activity to venture into innovative activity, and when they have to depend on small seed capital and cash flow to shoot themselves to the top in terms of attaining the set business performance, they fail. The startups face difficulty of accessing and utilizing external finance resources in case they want to pursue the advancements of technologies since there is a distinct risk to investments in early-stage Startups. It includes a great number of demonstrative and illustrative examples. Some of these are in blockchain, life science, energy, computing, aerospace, image tracking, virtual reality, etc. "Some more illustrative examples of deep tech technologies include, the use of artificial intelligence (AI) to forecast natural disasters or the use of molecular imaging technology to diagnose disease. The industries are characterized by a high round of research and development with long time to market and are not parallel to consumer technology or software as a service (SaaS). Their bargaining and social power is stupendous, and the AI market is estimated to cumulate to 1.8 trillion by 2030."[6] Nonetheless,

[3] Eliza Strickland, *The Turbulent Past and Uncertain Future of AI: Is There a Way out of AI's Boom-and-Bust Cycle*? IEEE Spectrum, 26–31. (2021).
[4] Byungki Lee, Byungchul Kim & Uladzimir V. Ivan, *Enhancing the Competitiveness of AI Technology-Based Stratups in the Digital Era*, 14 Admin. Sci. 6 (2024).
[5] Eun-ji Hyun & Byung-Tae S. Kim, *Overcoming Uncertainty in Novel Techonologies: The Role of Venture Capital Syndication Networks in Artificial IntelligenceStartup Investmnets in Korea and Japan, 12 Sysytems 72 (2024), https://www.mdpi.com/2079-8954/12/3/72*
[6] Elias Ketema Gebru and Abu Labib Mohammed Ashfaqul Awal, The Impact of Venture Capital on the Growth of Deep-Tech Startup: An Empirical Analysis on University Incubator Startup Exits (June 11, 2021) (unpublished

the problems of regulation e.g. privacy and ethical AI, safety, and export legislation are a drag on development and investment.

What is Deep-Tech and AI in the Venture Capital World: Opportunity and Regulations Issues

Deep tech is a term applicable to technologies that use important scientific or engineering innovations that may take years of development work prior to commercialization. "The BCG and Hello Tomorrow have stated that deep tech startups are based on a scientific being something found or something meaningful engineering innovation and taking part in working hard to combat large problems that genuinely make a difference to the world"[7]. Unlike the present-day tech startups, deep-tech startups are developed on the basis of the scientific and technical discoveries helping to find the solution to the problem with the global significance and resulting in the violation of the established rates. "In a survey carried out on the Global Startup Ecosystem (GSE) it was revealed that nearly 45 percent of the startups that are formed in 2019 were of the deep tech category whereas the same situation is that of the half figure in 2010 -2011."[8] A typical example of AI, which sometimes goes under deep-tech, includes systems that emulate human intelligences, machine learning systems that make predictions about human behavior, natural language processing that empowers language simulations such as Gork AI or ChatGPT, or computers that power self-driving cars. In contrast to consumer tech or software as a service, deep tech and AI are characterized by high, R&D driven development cost, time, and capital intensive. A consumer app may take a matter of months, a quantum computing startup may take a decade. The difference is that they are more risky bets for VCs but also they carry the temptation of paradigm transformative change. An example is, "Deepmind has solved the folding of proteins, which has a history of decades, and Quantumscape with its solid state batteries is promising to change the face of electric cars, whereas the most important transactions of 2025 include the activities of AI based platforms such as OpenAI, that raised a deal of 40 Billion dollars, and companies such as Tonbo imaging

M.S. thesis, KTH Royal Institute of Technology), https://www.diva-portal.org/smash/get/diva2:1588563/FULLTEXT01.pdf.

[7] Arnaud de la Tour et al., Deep Tech: The Great Wave of Innovation, Hello Tomorrow & Bos. Consulting Grp. (2021), https://hello-tomorrow.org/wp-content/uploads/2021/01/BCG_Hello_Tomorrow_Great-Wave.pdf.

[8] SG &Global Global Startup Ecosystem Report 2019 entrepreneurialhunt.com' Entrepreneurship Network, (Global Startup Ecosystem Report 2019) http://startupgenome.com/reports/global-startup-ecosystem-report-2019.

represent the deep learning thesis, having advanced hardware solutions."[9]

Regulation frameworks highly influence the creation of deep tech and AI. The EU and the U.S. have quite stringent data collection and use-related regulations in the form of the General Data Protection Regulation in the EU and the 'California Consumer Privacy Act in the U.S. Data healthcare falls under the control of the California Consumer Privacy Act and the Food and Drug Administration standards, which are issued by the federal government.'[10] The GDPR penalties are up to 20 million or 4 percent of the yearly turnover; this is an intimidating perspective to startups that are short of cash flow.[11] In Asia, there is the Digital Personal Data Protection Act (2023) of India, an added layer of compliance that startups must be prepared to comply with different legal requirements.[12] The EU AI regulation in the future (proposed AI Act, 2024 Draft) applies a risk-based system requiring transparency and fairness in high-risk systems such as hiring algorithms, facial recognition and others. Failure to comply would also lock out startups to the EU which is a 3.7 trillion economy. In America, the imagery here is also worrying, with New York introducing bias auditing of algorithms, requiring companies to demonstrate model fairness, which increases costs and complexity. China has placed a heavy emphasis on both state supervision and ethics relating to AI, and the limitations in export conditions in the U.S. entail restrictions in specific fields such as semiconductors and quantum computing. Such regulations bring about uncertainties such as delays in approval, cost of compliance and barriers to enter markets, which is not appealing to investors. Such deep tech as autonomous cars or medical AI are subjected to more strict safety requirements Waymo, an industry dominant in autonomous cars, focused on years of regulations by the states of the U.S and EU standards of safe operation and compliance cost more than $50 million. Liability is a grey matter In case of an incorrect diagnosis of a patient by AI diagnostic tool, who is liable? The applications of technologies such as quantum computing and chips dedicated to AI have certain restrictions when it comes to export. The United States. The EAR of Department of Commerce restricts the transfer of the sensitive technology which affects startups like PsiQuantum who shifted to EU markets to escape restrictions. These regulations leave the

[9] QuantumScape Stock Jumps on Solid-State Battery Progress, Perplexity AI (July 24, 2025), https://www.perplexity.ai/discover/top/quantumscape-stock-jumps-on-so-nfKnoXILRsO3vEeOhAHLyw.
[10] California Consumer Privacy Act (CCPA), CAL. OFF. ATT'Y GEN. (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa.
[11] Giovanni Sartor and Francesca Lagioia, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, EUR. PARL. DOC. (STOA) PE 641.530 (June 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.
[12] Gowree Gokhale et al., India's Digital Personal Data Protection Act, 2023: History in the Making, NISHITH DESAI ASSOCS. (Aug. 7, 2023), https://www.nishithdesai.com/NewsDetails/10703.

startups with global expansion hopes in uncertainty.

The laws make it unpredictable where approvals take long period, cost incurred which makes business be in compliance with dictates and the barriers of entry that act as deterrent factors in investment. By doing due diligence in giving capital to a venture capital, VCs have minimised the impact of the risk of the regulatory risk because they can even assess how prepared a new technology based startup is to meet regulatory scrutiny and how regulatory environments might impact these businesses too. Regulatory changes can be predicted by observing lawful and compliance alliances. When they arise, in-house policy groups at the Andreessen Horowitz can guide portfolio companies through regulatory snafus within a particular startup that are not at the point of imperiling the entire returns. It is tactical in the visioning of VCs in the sponsoring of innovation and the uncertainty is taken care of.

Protecting the Fire: The Application of Deep-Tech/Artificial Intelligence Startups in Safeguarding their Innovative Ideas which drive Innovation

Apparent in the modern world, artificial intelligence (AI) has a very significant influence when it comes to innovation. Artificial intelligence has brought about incredible opportunities and has led to the revolution of industries, including healthcare, finance industry, entertainment and manufacturing. It is not automation but re-engineering of new avenues in advancement. The days when innovation has no boundaries belong to the AI era. The concepts created in one region of the world may be massively influencing the whole world. AI requires networked collaboration and engagement on an international level to get the most out of it. The processing and analysis capability of AI enabled businesses and researchers to look deeper into issues characterized by tons of data. Whether it is healthcare and financial industries, marketing and climate science, AI is assisting us to have a better decision-making process, and so far we find a pattern that previously remained unseen.

The benefits of a moat against competition can be provided by any piece of technology as unique as in the field of medical diagnostics with AI power or computing with quantum technology. A good example here is 'a startup like xAI, with an AI solution like Gork, and how they share all the same to add as other similar companies like OpenAI, the only distinction is that it has proprietary algorithms.'[13] VCs consider good IP protection to be long-term value.

[13] xAI, *xAI* (Aug. 14, 2024), https://web.archive.org/web/20240814*/https://x.ai

Weak IP strategy may scare investment particularly in the regulatory intensive sectors where the regulatory risk (compliance) increases the uncertainties. Such legislation as the EU AI Act or U.S export controls on sensitive technologies (i.e., semiconductors) obligates IP protection by startups in their IP in forms that do not violate data privacy, transparency and national security regulations. Lack of compliance with these regulations may result in the exclusion of the IP strategies in the market or make the companies liable. Deep tech and AI innovation consists of iterative problem solving, which is powered by creativity. An example is a startup working on an AI that can model climate and it will always need to be updated on new data sources in order to perfect its algorithms. Excessive intellectual policy, like locking down all creativity, or inadequate protection which can end up being idea theft may kill team work and even experimentation. There is a balance to be achieved by start-ups to exercise an innovative culture and protect their breakthroughs.

Innovative technologies such as AI algorithms in natural language processing or cocaine solid-state batteries (i.e., deep-tech) hardware tend to be secured with the usage of patents. To illustrate, "the deep-tech company, QuantumScape, has over 200 patents of battery technologies, and thus, it will secure its position in the electric vehicle industry."[14] However, patents are expensive (it costs over 50,000, and there is the open disclosure of information) which may not fit in the fast evolving sectors of AI, where inventions become obsolete overnight. Patent business is a well calculated decision of what patent to pick by the start-ups and they usually take a gamble on basic technologies that have some long term values. Trade secrets are already the order of the day with AI startups, who are protecting innovations, which are considered sensitive, including proprietary training datasets and models. Anthropic, one of OpenAI competitors has kept the methodologies of its training of AI algorithms within the confines of business secrets not to share them. It also requires a high degree of internal controls including non-disclosure agreements, data security and employee training on the subject of confidentiality. A code, user interfaces, documentation of the software are covered with the copyright along with the identity of the brand which is covered with the trademark. In order to build awareness of the autonomous vehicle on the market, a new business like Waymo can trademark its name and copyright software interface. These tools have a lesser application in deep-tech although they may be used to support other IP application. Taking into consideration

[14] Zouina Karkar, Mohamed S. E. Houache, Chae-Ho Yim & Yaser Abu-Lebdeh, Industrial Perspective and Intellectual Property Landscape on Solid-State Battery Technology with Emphasis on Solid-State Electrolyte Chemistries, 10(1) BATTERIES 24 (2024), https://www.mdpi.com/2313-0105/10/1/24.

the universal coverage of AI and deep-tech market, startups are obliged to operate with various IP regulations. To highlight the argument, patenting the AI in China is far more secure than it is in some of the emerging economies. Quantum startups (e.g. PsiQuantum) patent in countries with large economies (e.g. U.S., EU), in order to gain market wide coverage without having the patent right in countries with high costs to enforce the rights.

Some put out peripherals rather than fundamental technology, hoping that it will attract attention and people will use it hence preserving the important intellectual commerce. As an illustration, 'Meta AI did not open source its entire LLaMA models, although attempting to develop developer communities around its models, it did not open source more advanced systems.'[15] It is an exchange which results in creativeness by creating competitive advantages and guarding them through working together. The most common approach here, startups normally sell the title of their technology to a bigger company or research organization and they still receive revenue, however these companies do not own the IP products. A good example is a biotech start up that was working on AI based drug discovery and licensed out its platform to the pharmaceutical behemoth and all agreements are related there including the specific safeguards to the algorithms in question. These types of partnerships also help realise easier leverages by way of regulatory complexities that would otherwise have been fueled by the partners in relation to compliance. In some situations where patenting may not be effective, the startups are expected to publish the non seminal innovation in an attempt to avert the patenting of some related innovations that may be financed by other parties. That is how certain AI startups were run, so that freedom of operations and investment in core IP was the main two aspects of focus to obtain investments.

Regulations and Compliance to Data Usage: Handling Privacy and the use of Artificial Intelligence Regulations in Different Nations

Artificial intelligence is no longer an innovative technology but is used everywhere and everywhere it makes an impact on our virtual communications and even critical choices in all areas. The uncontrolled possibilities of AI have created actual ethical, legal, and cultural concerns as incidences happening around the world have indicated that governance is necessary. AI-enabled surveillance technology that threatens privacy and AI algorithms that

[15] Harry Guinness, Meta AI: What is Llama 4 and Why Does it Matter? ZAPIER (Apr. 8, 2025), https://zapier.com/blog/llama-meta/.

unwittingly discriminate in hiring are only two perfect examples that have raised the discussion on the appropriate use of AI around the globe. Trust is the guiding principle of any technological implementation process, and as such, the potential of AI can easily be forced into a situation of people distrusting the technology because no one held them accountable.

Data governance is one of the most important measures of the efficient management of data. Data governance is the activity of creating and applying regulations, policies, and other forms of protective harm against sensitive information. It is the role of our system to make sure that the data will be reliable, available and controllable throughout its life. The steps of introducing the AI technologies, such as machine learning algorithms, into the business and automating business process, obtaining insights, and making data-driven decisions are referred to as AI integration. The way data governance can be transformed with the help of IA is that in case data categorisation, access control, and risk assessment capabilities could be effectively simplified through the use of automated workflows, organisations could streamline them effectively. This allows companies to handle their valuable data with the most efficiency and accuracy but it is also vital to take note of ethical considerations, compliance needs and danger of biassed or discriminatory results when using AI in data governance. Governments across the world are taking initiatives to solve these issues:

- **European Union: GDPR and the Artificial Intelligence Act (AIA)**

The General Data Protection Regulation (GDPR) of the European Union, which went into effect in 2018, is the most extensive and significant data protection law worldwide. Core principles of data processing including data minimisation, purpose limitation, and storage limitation are mentioned in Article 5[16]. Six legitimate grounds for processing personal data are outlined in Article 6[17] i.e Consent under Article 6(1)(a), Contract under Article 6(1)(b), Legal Obligation under Article 6(1)(c), Vital Interests under Article 6(1)(d), Public Task under Article 6(1)(e), and Legitimate Interests under Article 6(1)(f) are the most frequently invoked criteria for the majority of venture capital-funded AI companies. Particularly pertinent to AI startups developing algorithms that handle user data is Article 25[18] providing Data Protection by Design and by Default which requires organisational and technical precautions right away.

[16] General Data Protection Regulation, 2018, art. 5.
[17] General Data Protection Regulation, 2018, art. 6.
[18] General Data Protection Regulation, 2018, art. 25.

In addition to GDPR, the EU is completing the Artificial Intelligence Act (AIA), a groundbreaking law designed to regulate AI systems according to risk classification. The AIA makes a distinction between AI systems that are prohibited, high-risk, limited-risk, and minimal-risk. Strict compliance measures, such as algorithmic transparency, human oversight, and data quality standards, will apply to high-risk systems (such as biometric identification, healthcare diagnostics, and credit scoring). The cost of compliance will increase significantly for startups creating or implementing such systems in the EU since they must guarantee conformance assessments, model documentation, and post-market monitoring. VC investors are now required to consider a startup's regulatory burden under the AIA and GDPR in addition to its technical merit.

- **India: The Digital Personal Data Protection Act, 2023**

Recently, India, one of the world's biggest digital markets, passed the Digital Personal Data Protection (DPDP) Act, 2023. In addition to consent requirements, data fiduciary obligations, and a central Data Protection Board for enforcement, the Act establishes a rights-based framework for processing personal data. Despite being influenced by GDPR, the DPDP Act has a more straightforward and adaptable framework that seeks to strike a balance between innovation and regulation. The Act imposes legal requirements on AI and deep-tech businesses that work with or process Indian data in relation to purpose limitation, notice and consent, data breach reporting, and cross-border transfer regulation (through jurisdictions that have been approved by the government). Both consumer-facing models and back-end AI data pipelines are impacted by these provisions. Compliance with the DPDP Act is becoming a crucial investment condition from the standpoint of venture capitalists. It is now part of legal due diligence to analyse third-party data-sharing contracts, consent procedures, grievance redressal systems, and privacy policies. It further puts limitations on cross-border data transfers under Section 16[19], data minimisation, purpose limitation, and consent-based data processing under Section 6[20]. Businesses with limited resources face serious financial risks due to the possibility of fines of up to INR 250 crore for noncompliance. There is uncertainty brought about by the DPDP Acts implementation requirements, which are still being developed as of July 2025, especially for AI startups that handle sensitive personal data. Furthermore, Section 4[21] mandates the requirement of explicit, revocable, and informed consent before collecting

[19] Digital Personal Data Protection Act, 2023, §16.
[20] Digital Personal Data Protection Act, 2023, §6.
[21] Digital Personal Data Protection Act, 2023, §4.

personal data. Section 7[22] authorises processing without permission for public interest, emergencies, or state functions. Section 9[23] designates specific companies as "Significant Data Fiduciaries," necessitating frequent audits and Data Protection Officers (DPOs) and Section 13[24] gives the government the power to alert countries that are allowed to trade data internationally.

- **United States: Sectoral and State-Led Data Laws**

A comprehensive federal data protection law does not exist in the United States. Rather, sector-level models (HIPAA for health, GLBA for finance) and state-level legislation like the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) control data governance. Enforcing "unfair and deceptive practices" in data usage is one way the Federal Trade Commission (FTC) contributes significantly. Although it will take a less centralised approach than the EU, recent executive orders and frameworks like the AI Bill of Rights and the NIST AI Risk Management Framework indicate the U.S. government's determination to move towards formalised AI regulation[25]. For venture capitalists, the United States poses a significant amount of legal ambiguity, requiring a case-by-case assessment of jurisdiction-specific compliance (such as California, Colorado, and Virginia). Startups should be ready for a patchwork of compliance rules if they plan to develop globally or pursue federal contracts.

The rights to access, deletion, correction, and data portability are outlined in Section 1798.100–115. The right to refuse the "sale" of personal information is granted by Section 1798.120. "Unfair or deceptive acts" are punishable under the Federal Trade Commission Act, 15 U.S. Code Section 45. AI startups risk legal repercussions if they make fraudulent claims on bias mitigation or data anonymisation. 'In re Everalbum Inc., FTC penalized Everalbum for deceptive use of facial recognition AI and failing to delete user data after consent withdrawal as per 15 U.S. Code § 45.'[26]

This generation of AI rules is significant because it establishes the parameters for innovation.

[22] Digital Personal Data Protection Act, 2023, §7.
[23] Digital Personal Data Protection Act, 2023, §9.
[24] Digital Personal Data Protection Act, 2023, §13.
[25] Nat'l Inst. of Standards & Tech., Artificial Intelligence Risk Management Framework (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.
[26] In re Everalbum Inc., FTC (2021)

In the modern business environment, regulatory compliance is not only a checkbox; rather, it is a strategic need. A competitive edge may be gained by those that proactively adjust to these standards, positioning themselves as reliable participants in a market that is becoming more and more scrutinised. Conversely, companies who ignore these trends run the danger of facing fines, harm to their brand, or even exclusion from markets.

VCs approaches to reduce Regulatory Risk: include investing in Deeper Tech and Artificial Intelligence

Of the start-ups in the current context 9 out of 10 do not survive and of the other 10 of survival and survival, 10 are becoming superrich to the venture capitalists. VC companies are those that offer money to the corporations that would transform the world as opposed to stores. They can discuss examples of this on Facebook which was just a site on the internet where students would criticize the beauty of the students. This preceded a swarm of venture capitalists who saw the incalculable potential of the social media network and poured a lot of money into the social media. Its current ex-market valuation of facebook is regarded as a gambling bet that would be dubious to take by venture capitalist and it sums to 1.43 trillion at the present moment. VC firms do not know the type of issues that need to be addressed because it is not known to the VC firms themselves, thus it is hard to come up with a method of handling the risk. When a firm is equipped with an estimation of the dangers it faces, it stands a better opportunity of making the tradeoffs between the drawbacks and benefits that it suffers in the venture financing procedure. The field of deep-tech and artificial intelligence (AI) innovation is a fast evolving target market in which venture capital firms have given much consideration to since the field has disruptive potential and exponential scalability.

Despite the fact that, the rapid pace of development of these technologies against the backdrop of limited development of laws and regulations, there is much uncertainty related to issues of data protection, algorithmic accountability, data transfers across national borders, ownership of intellectual property (IP), and ethical governance of AI. These legislative uncertainties carry with them financial, operational and reputational risks, and also present a problem of compliance with the investors who have specified their risk toleration levels and their exit timelines. To this end, the venture capitalists ought to implement sound risk mitigation initiatives which are apt to fuel growth and expansion of the firms they invest in besides being compatible with the regulatory framework which is dynamic.

Regulatory Challenges in Deep-Tech and AI

Startups in the deep tech and artificial intelligence sectors confront numerous regulatory obstacles that make venture capital investments more difficult. India's regulatory environment poses unique difficulties in addition to global issues. Legislative frameworks are frequently outpaced by the quick speed of technology innovation, which poses serious risks:

1. **Intellectual Property (IP) Uncertainties:** AI-generated ideas raise issues about inventorship, patentability, and ownership, challenging established intellectual property frameworks like the European Patent Convention and the U.S. Patent Act (35 U.S.C. § 101). For example, the U.S. Patent and Trademark Office's position that AI is a non-human inventor leads to legal ambiguity, which puts businesses at danger of invalidation and IP conflicts. In India, computer programs themselves are not patentable under Section 3(k)[27] of the Patents Act, 1970, which leaves AI algorithms unclear and raises the possibility of IP disputes which puts startups at danger of invalidation.
2. **Data Privacy and Compliance:** Strict laws that place strict requirements on data collection, processing, and storage include the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) in the EU (Regulation (EU) 2016/679). Operational disruptions and significant fines of up to 4% of yearly global turnover are possible consequences of non-compliance with GDPR, especially for AI models that depend on massive datasets. In India, data fiduciaries are subject to strict requirements under the DPDP Act, which include consent procedures and data minimisation and non-compliance can result in fines of up to INR 250 crore. As in Justice K.S. Puttaswamy v. Union of India[28] case recognised privacy as a fundamental right under Article 21 of the Constitution, laying the constitutional foundation for the DPDPA.
3. **Ethical and Bias Concerns:** New laws, like the EU's AI Act, require AI systems to be transparent, accountable, and bias-free. Non-compliance puts a company at risk for fines and negative publicity, particularly in delicate industries like healthcare and finance. The lack of AI-specific legislation in India increases dangers because organisations like the Ministry of Health and the Reserve Bank of India (RBI) are looking into ethical issues including algorithmic bias in industries like healthcare and finance.

[27] Patent Act, 1970, §3(k).
[28] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.

4. **Issues with Intellectual Property Ownership and Enforcement:** While traditional IP regimes presume human inventorship, deep-tech ventures frequently produce innovative inventions. In most jurisdictions, it is still unclear what the legal status of inventions created by AI is. Additionally, companies might use open-source software, government-funded research, or collaborative R&D, which raises questions about fragmented ownership or license violations. The lack of a strong, defendable IP portfolio lowers a startup's valuation in the eyes of venture capital firms and jeopardises possible exit plans.
5. **Jurisdictional Variability:** Startups that operate internationally have compliance challenges due to differing regulatory approaches between jurisdictions, such as China's centralised Cybersecurity Law and the United States' disjointed state-level data rules. In India, sector-specific guidelines (such as the RBI's fintech regulations) and overlapping regulations (such as the Information Technology Act, 2000) make compliance more difficult for startups that operate internationally or across states.

VC Strategies for Risk Mitigation

1. **Compliance with Data Protection and Privacy:** Large-scale data collection and processing are frequently used by AI firms to train algorithms and increase model accuracy. Due to this approach, they fall under the purview of international data privacy regulations, including India's DPDP Act and the European Union’s GDPR. Strict guidelines for user consent, purpose limitation, data minimisation, and cross-border data transfer are required under these rules. Failure to adhere to these frameworks may result in severe sanctions and harm to one's reputation. These risks directly jeopardise the scalability and legal viability of the businesses in an investor's portfolio.
2. **Enhanced Due Diligence:** VCs carry out IP audits across the world to confirm patent validity and ownership. To make sure AI breakthroughs are eligible as patentable subject matter, audits in India concentrate on adherence to Section 3(k) of the Patents Act, 1970. In India's competitive IT sector, VCs evaluate freedom-to-operate to reduce the risk of infringement claims. VCs should assess compliance with international standards such as GDPR, paying particular attention to permission frameworks, data governance policies, and breach procedures. In India, adherence to Section 16[29] of the Act's data localisation and cross-border transfer regulations is essential since noncompliance carries hefty penalties. In order to ensure compliance with international standards and India's IT Rules, 2021,

[29] Digital Personal Data Protection Act, 2023, §16.

venture capitalists evaluate the risks posed by third-party vendors, including cloud providers.

3. **Algorithmic Responsibility and Sector-Specific Law:** Increased regulatory scrutiny may be imposed on startups using AI in delicate industries like healthcare, finance, or education. Regulations like the EU Artificial Intelligence Act categorise AI systems according to their level of danger, placing more stringent compliance requirements on "high-risk" applications. These include responsibilities for post-deployment monitoring, bias testing, algorithmic explainability, and data governance. These compliance expenses must be taken into consideration by VC companies when assessing a startup's long-term prospects and operational feasibility.
4. **Contractual Safeguards:** Startups around the world compensate VCs for intellectual property and legal losses. In India, provisions addressing fines for data breaches or intellectual property issues are covered by the Patents Act, 1970, and the DPDP Act. For instance, VCs are protected by up to INR 250 crore in indemnity for DPDP Act violations. Startups should be required to abide by both Indian and international rules, especially those pertaining to AI-driven fintech. Remedies for warranty breaches should include sector-specific fines, as those imposed by SEBI on AI-powered trading platforms, and equity adjustments.

Future Outlooks: Evolving Laws and its Consequences on Deep-Tech/AI Startup Industries

Deep-tech and AI innovation is based on intellectual property rights, since companies use trade secrets, copyrights, and patents to safeguard proprietary algorithms, datasets, and technological procedures. However, unclear IP ownership presents serious problems, especially for outputs produced by AI. Because these assets improve valuation and competitive posture, investors give preference to firms with strong intellectual property portfolios. But the absence of a well-defined legal precedent for AI-generated intellectual property raises the perceived risk and may discourage funding. For startups to reduce risks and draw in funding, proactive IP strategies are necessary. One such strategy is obtaining patents for human-led processes that support AI development.

The global venture capital (VC) scene has changed dramatically as a result of the exponential expansion of deep-tech and artificial intelligence (AI) innovations. Investors have never-

before-seen potential with startups at the nexus of deep technology and artificial intelligence (AI). But these companies also cross regulatory boundaries that have never been explored before, particularly in the areas of algorithmic accountability, data privacy, and intellectual property (IP). As national and international legal frameworks are unable to keep up with the rate of innovation, the changing regulatory environment is starting to change how startups operate and how investors approach their investments.

1. Data Privacy and Security Regulations:

Despite the fact that data is essential to AI businesses, strict data privacy laws, such the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) of the European Union, entail substantial compliance requirements. The GDPR requires specific agreement before processing data and penalises noncompliance with fines of up to 4% of annual global turnover. For deep-tech startups that work with sensitive data, like biometrics or healthcare, these rules can be expensive and difficult to comply with.

Further complicating the operational environment for startups are new legislation that create extra requirements for data exchange and interoperability, such as the EU's Data Act (2023). These rules have the potential to restrict access to data, which is a vital resource for AI model training, which would stifle innovation. Startups that use synthetic data to lessen their need on personal data and incorporate privacy-by-design principles will be better equipped to overcome these obstacles and obtain capital.

2. Ethical AI and Regulatory Oversight:

Deep-tech startups now face an additional level of complexity due to the emergence of ethical AI regulations, such as the EU's Artificial Intelligence Act (AIA). By 2026, the AIA will have been fully implemented. Significant financial risks for startups arise from non-compliance, which can result in fines of up to €35 million or 7% of global turnover. These rules affect every stage of the startup process, from development to launch. Startups, for instance, have to make sure that AI decision-making procedures are transparent and carry out thorough impact evaluations, which might raise expenses and postpone product launches. The AIA's rules raise the bar for due diligence for VC investors, who must evaluate a startup's capacity to adhere to moral AI principles while preserving scalability. In State v. Loomis[30], the court used a

[30] State v. Loomis 337 U.S. 241, 251 (1949).

proprietary AI-based risk assessment tool (COMPAS) in sentencing. While the decision was upheld, it triggered global concerns about algorithmic transparency, fairness, and due process, which aligns perfectly with your ethical concerns and AIA risk classification discussion. By proactively implementing ethical AI frameworks, including those that are in line with IEEE's Ethically Aligned Design principles, startups can stand out in a crowded industry and attract more investors.

3. Implications for VC Investment Strategies:

Deep-tech and AI startups' VC investment strategies are greatly influenced by the changing regulatory environment. Startups with defined compliance roadmaps are becoming more and more popular with investors since regulatory infractions can damage market trust and result in losses. As per a Pitch Book poll conducted in 2024[31], 62% of venture capital firms now see regulatory compliance as a crucial factor when making investment selections.

Additionally, regulatory ambiguities present chances for operational distinction. A competitive advantage can be gained by startups that foresee regulatory changes, such as by creating accountable AI models to adhere to the AIA. Venture capital firms are also looking into new funding methods like regulatory sandboxes, which let startups test their ideas under regulatory supervision in restricted settings. Supported by countries like Singapore and the UK, these sandboxes allow startups to scale their operations while proving compliance, which attracts risk-averse investors.

With the help of programs like the NDTSP, regulatory sandboxes provide an alternative by enabling startups to test innovations in safe settings. VC firms find these sandboxes appealing because they allow startups to show compliance while growing. Another example of how VC investments are coordinating with government-backed innovation ecosystems to de-risk deep-tech ventures is the Mounttech Growth Fund's collaborations with college incubators.

4. The Shifting Regulatory Terrain: From Laissez-Faire to Proactive Oversight

In the past, the regulatory environment for AI and deep-tech startups was comparatively liberal. These companies were able to experiment and iterate quickly due to regulatory loopholes and

[31] PitchBook Data, Inc., *Global VC Outlook 2024: Regulation as a VC Consideration* (Jan. 2024), https://pitchbook.com/news/reports/global-vc-outlook-2024.

legal ambiguities. Nonetheless, regulatory bodies throughout the world have started strong legislative interventions in response to data exploitation scandals (like Cambridge Analytica), worries about algorithmic opacity, the emergence of deepfakes, and the misuse of generative AI.

Among the most notable of these is the Artificial Intelligence Act (AIA) of the European Union, which assigns stringent compliance requirements to "high-risk" systems and categorises AI applications according to risk levels. While there is currently no overall AI legislation in India, sectoral regulations under the Information Technology Act of 2000, the DPDP Act, and domain-specific policies are becoming more and more relevant to businesses that use AI. The United States has embraced a decentralised approach, with the National Institute of Standards and Technology (NIST) and the Federal Trade Commission (FTC) providing guidelines. Particularly in the Global North, these legislative changes from reactive to anticipatory legislation are having an impact on how deep tech and AI businesses develop their products and control risk.

5. Data Governance and Sovereignty: A Legal Minefield

Geopolitical actors and privacy regulators are closely monitoring the monetisation of data, which is frequently the most valuable asset of an AI business. Cross-border transfer limits, permission procedures, and extraterritorial data requirements are introduced by laws such as the General Data Protection Regulation (GDPR) of the EU and the DPDP Act, 2023 of India. The following are important regulatory tensions:

- **Mandates for Data Localisation:** Countries such as China and India are pushing for data localisation in fields that are considered sensitive or important (e.g., defence, fintech, health). Compliance frequently means significant compliance costs and rewriting backend infrastructures, which affects scalability and investor confidence for firms that use cloud infrastructure and global databases.
- **Purpose Limitation and Algorithmic Training:** The fundamental technique of iterative model training is incompatible with the concepts of purpose limitation enforced by laws such as GDPR. AI startups are subject to regulatory scrutiny and must defend the reuse of data in training loops, which frequently lacks legal precedent.
- **Bias, Discrimination, and Explainability:** Mandatory transparency rules for algorithms are being introduced by the EU AIA and U.S. state regulations, especially

in sensitive use cases like healthcare, credit rating, and employment. Startups may now have to prove that their models are equitable and comprehensible, a requirement that is still unclear from a technical and legal standpoint.

Early-stage start-ups' capital and operating costs rise as a result of these compliance requirements, which also make them less appealing to venture capitalists seeking quick scalability and cost-effectiveness.

6. Regulatory Impact on VC Investment Patterns and Exit Strategies

VC behaviour is being recalculated by the evolving legal environment. Investors use regulatory due diligence as a pre-investment filter and include legal risk as a critical value indicator. A few effects are:

- **Jurisdictional arbitrage:** Investors are giving preference to businesses that are based in countries with clear or advantageous AI and IP laws (such as Singapore, Estonia, and several U.S. states), which encourages regulatory arbitrage.
- **Delays in Deployment and Valuation Haircuts:** Startups that operate in highly regulated or unpredictable contexts may encounter discounted values or delays in funding tranches. A startup in India that uses private health information, for example, would be valued lower if it doesn't have strong DPDP Act compliance systems.
- **Transition from B2C to B2B Models:** Because consumer-facing AI applications (like facial recognition and health tech) are disproportionately impacted by regulatory uncertainty, venture capitalists prefer business-to-business (B2B) models that use enterprise-level AI solutions with more transparent legal accountability chains.
- **Exit Strategy Changes:** Now, especially in the US and the EU, public listings (IPOs) of AI startups are subject to stringent regulatory scrutiny. As a result, a lot of venture capitalists are planning their exits by acquiring larger tech companies that are better able to withstand regulatory scrutiny.

Conclusion

With deep-tech startups and AI startups pushing further on the boundaries of what can be done, venture capital has become not only a source of investment but a strategic asset throughout the complex maze of legislation. These companies often work in areas that support long gestation times, high capital requirements and breakthrough capacities but are also susceptible to increasing international regulations. AI and deep tech have transited proactively into an area of

permissive regulation between the EU and its GDPR and Artificial Intelligence Act, India, and its DPDP Act, and the patchwork domestic regulation aspect in the United States. This change presents great challenges to companies willing to expand, despite the fact that it is an attempt to bring accountability, safety, and justice. Venture capitalists are now paying attention to legal issues when it comes to investing and consider due diligence, data, governance, intellectual rights and ethical alignment with AI as a priority. Nowadays, the success of a startup relies not only on its technology advancement but also on its ability to interpret the tendencies of legislature, follow the requirements and regulations that follow jurisdiction, and develop respectable privacy framework. IP strategies have taken the form of trade secrets and patents as well as through licensing and open-source quasi-hybrids, all of which have proved to be important tools in risk mitigation and long-term value-preservation. Also, such mechanisms as government-supported innovation hubs and regulatory sandboxes contribute to the shift as it allows entrepreneurs to undergo testing in an unregulated environment and provides venture capitalists with a guarantee of compliance with regulations. What lies ahead in the future of innovation financing can certainly be said to be conditioned by this interface between entrepreneurial flexibility and legal know-how. Compliance is part of core goals of the startups that do not view it as an obstacle; such an approach will attract consistent financing and will create a force to influence the development of responsible technology as regulations evolve. It is the process of protecting the validity of innovation, its scalability as well as the societal value within this high-stakes arena, not just the process of contributing to it.