Page: 517-546 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 1

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.24

ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN ANALYTICS IN DETECTING CRYPTO TAX EVASION

Vidushi Singh Vihan[1] & Dr.Afreen Almas[2]

I. ABSTRACT

This paper examines how artificial intelligence (AI) and blockchain analytics can be operationalised as enforcement technologies to detect crypto tax evasion in India, while remaining compliant with evolving legal constraints on privacy and digital evidence. It situates the analysis within India's post-2022 "virtual digital asset" (VDA) taxation architecture, including the statutory definition of VDA, the special charging and ring-fencing framework that taxes transfers at a flat rate with limited deductions, and the transaction-level reporting trail created through the one per cent tax deduction at source (TDS) mechanism on VDA transfers. It further maps the parallel expansion of anti-money laundering coverage to VDA service providers and explains how these compliance streams generate high-volume, high-granularity datasets suitable for automated risk scoring. On the technology side, the study details how blockchain forensics converts raw ledger data into investigable transaction graphs through address clustering, attribution, taint tracing, and typology-based risk signals, and how AI systems use these features to detect anomalies such as non-reporting, under-reporting, misclassification, offshore routing, chain-hopping, privacy-enhancing obfuscation, and circular or undervalued intra-group transfers. It argues that integrated models combining on-chain traces with off-chain records (exchange KYC, TDS data, FIU reports, and other regulatory filings) can reconstruct undeclared trading histories and prioritise cases with higher revenue risk more effectively than manual scrutiny.

[1] PhD Scholar, Sardar Patel Subharti Institute of Law, Swami Vivekanand Subharti University (India). Email: vidushivihan@gmail.com
[2] Assistant Professor, Sardar Patel Subharti Institute of Law, Swami Vivekanand Subharti University, Meerut (India).

II. KEYWORDS

Artificial Intelligence (AI) in Tax Enforcement, Blockchain Analytics and Crypto Forensics, Virtual Digital Asset (VDA) Taxation Framework, Crypto Tax Evasion Detection Techniques, AML and Digital Evidence Governance

III. INTRODUCTION

A. Background of Crypto Assets and the Rise of AI driven Enforcement

Crypto assets started as a niche experiment in peer to peer electronic cash but they now cover payment tokens, exchange tokens, stablecoins, NFTs and DeFi governance tokens that move on distributed ledgers without central intermediaries.[3] Indian policy makers watched this growth for a decade while the market deepened, and then they created a distinct category of "virtual digital asset" and a ring-fenced regime for taxing its transfers at a flat 30 per cent rate with strong limits on deductions and loss set off.[4]

The new provisions in the Income Tax Act 1961 treat most cryptocurrencies and many NFTs as VDAs while they still deny them the status of legal tender, so they try to tax without fully recognising them as money.[5] Budget speech material links this special treatment with a "phenomenal increase" in VDA trading volume and with worries about unreported gains, which shows that tax enforcement concerns already shape the legal architecture at the policy level.[6] Yet peer to peer trading, self-hosted wallets and informal broker networks continue to make non reporting, under reporting and misclassification of crypto gains quite easy in practice.

Parliament also built a parallel reporting trail through section 194S, which requires a 1 per cent TDS on consideration for VDA transfers and thus generates large volumes of

[3] Byomkesh Panda, Taxation of Virtual Assets 1–3 (Nat'l Acad. of Direct Taxes 2024), https://nadt.gov.in/writereaddata/MenuContentImages/TAXATION%20OF%20VIRTUAL%20ASSETS638701452732833757.pdf (last visited Feb. 14, 2026).
[4] Id. at 4–7.
[5] Income Tax Act, 1961, § 2(47A) (India).
[6] Nirmala Sitharaman, Minister of Fin., Budget 2022–2023 Speech ¶ 131 (Feb. 1, 2022), https://www.indiabudget.gov.in/doc/bspeech/bs202223.pdf (last visited Feb. 14, 2026).

transaction level data that the administration can mine for risk.[7] Recent professional commentary points out that taxpayers still route trades across several exchanges, use offshore platforms and book some holdings as long term investments while they actually trade in the short term, so traditional manual scrutiny of returns and information statements cannot keep pace with the complexity of these patterns.[8]

B. Research Questions

1. How can artificial intelligence–driven blockchain analytics be legally integrated into India's Virtual Digital Asset taxation framework to enhance the detection, investigation, and prosecution of crypto tax evasion without violating constitutional safeguards and statutory due process requirements?
2. To what extent do existing Indian legal regimes, including the Income Tax Act, 1961 (as amended for VDAs), the Prevention of Money Laundering Act, 2002, and the Digital Personal Data Protection Act, 2023, adequately regulate the use of AI-based crypto forensic tools in tax enforcement and financial intelligence operations?
3. What are the evidentiary challenges and admissibility standards associated with AI-generated blockchain forensic outputs under the Bharatiya Sakshya Adhiniyam, 2023, particularly in establishing attribution, transaction tracing, and proof of tax liability in crypto-related offences?
4. How can regulatory coordination between tax authorities, financial intelligence units, and virtual asset service providers be strengthened through AI-enabled analytics to address cross-border crypto tax evasion while ensuring compliance with international taxation norms and data governance principles?

[7] Income Tax Act, 1961, § 194S (India).
[8] Shalini Nagar, Virtual Digital Assets under Direct Taxation, Chartered Sec'y, Apr. 2025, at 18, 20–22, https://www.icsi.edu/media/webmodules/CSJ/April-2025/12.pdf (last visited Feb. 14, 2026).

C. Research Objectives

1. To examine the legal and regulatory framework governing the taxation of Virtual Digital Assets in India, with specific focus on statutory provisions relating to income computation, reporting obligations, TDS compliance, and enforcement mechanisms under the Income Tax Act, 1961.
2. To analyse the role, operational mechanisms, and effectiveness of artificial intelligence and blockchain analytics tools in detecting patterns of crypto tax evasion, including transaction tracing, risk profiling, and forensic attribution.
3. To evaluate the evidentiary validity, admissibility standards, and procedural safeguards associated with AI-generated blockchain forensic outputs under the Bharatiya Sakshya Adhiniyam, 2023, and related principles of digital evidence law.
4. To assess the interface between crypto tax enforcement technologies and allied legal regimes, including anti-money laundering compliance under the Prevention of Money Laundering Act, 2002, and data governance obligations under the Digital Personal Data Protection Act, 2023.

D. Research Methodology

This study adopts a doctrinal (black-letter) research methodology focused on the systematic analysis of primary legal sources governing Virtual Digital Asset taxation and technology-enabled enforcement in India. It undertakes close textual interpretation of the Income Tax Act, 1961 (as amended to introduce the VDA taxation and TDS framework), the Prevention of Money Laundering Act, 2002 and allied rules extending compliance to VDA service providers, the Bharatiya Sakshya Adhiniyam, 2023 for standards of electronic evidence and proof, and the Digital Personal Data Protection Act, 2023 for lawful processing, purpose limitation, and security obligations in data-driven investigations.

The research further analyses delegated legislation, CBDT notifications/circulars, FIU-IND directions, and relevant judicial precedents to identify legal thresholds for attribution, admissibility, and procedural fairness when AI and blockchain analytics are used for detection and investigation. Secondary sources such as authoritative commentaries, academic literature, technical standards on blockchain forensics, and policy reports are used to contextualise doctrinal findings and to evaluate the coherence, gaps, and enforceability of the current framework. The methodology culminates in normative legal reasoning to derive reform proposals that align enforcement capability with constitutional safeguards, evidentiary reliability, and data governance requirements.

IV. CONCEPTUAL AND TECHNOLOGICAL FRAMEWORK

A. Crypto Assets, Virtual Digital Assets and Tokens – Legal and Technical Definitions

Crypto assets link code and value because they embed rules of creation and transfer inside distributed ledgers instead of a central server. In practice, lawyers and engineers use "crypto asset" as a wide label for any cryptography-based representation of value that parties can hold or move on a blockchain without an intermediary.[9] Work of international tax bodies treats crypto assets as a separate asset class with distinct issues of valuation, traceability and reporting.[10]

Indian law does not define "crypto asset" in general terms but creates the statutory category of "virtual digital asset" to catch most tokens that Indian residents trade. Section 2(47A) of the Income Tax Act 1961 describes a VDA as any information, code, number or token, other than legal tender, generated through cryptographic means or otherwise,

[9] OECD, Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues 15–18 (2020), https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/taxing-virtual-currencies_e787d5db/e29bb804-en.pdf (last visited Feb. 14, 2026).
[10] OECD, International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting Standard 21–24 (2023), https://doi.org/10.1787/896d79d1-en (last visited Feb. 14, 2026).

which gives a digital representation of value that users can transfer, store or trade electronically.[11] The clause also covers NFTs and other digital assets that the Central Government may notify, which keeps the definition technology neutral and lets new token forms fall into the tax net without new primary legislation.

Market participants speak of "tokens" when they mean the discrete units that a protocol or smart contract issues and records as balances on blockchain addresses. A simple functional taxonomy separates payment or exchange tokens, utility tokens and investment or asset referenced tokens, depending on whether a token mainly works as money, as an access key to a network, or as a claim on some underlying pool of assets or rights. Comparative regimes such as the EU Markets in Crypto Assets Regulation adopt similar categories and define "crypto asset" as a representation of value that uses distributed ledger technology, while carving out instruments already covered by other financial law.

B. Fundamentals of Blockchain Ledger, Transaction Traceability and Pseudonymity

A blockchain ledger records transactions in ordered blocks that link through cryptographic hashes, so each new block depends on the integrity of the entire prior chain. Network nodes validate candidate blocks under a consensus rule such as proof-of-work or proof-of-stake and then replicate the accepted ledger across many machines, which makes later alteration extremely hard in practice.[12] This technical design gives regulators and courts a time-stamped, tamper-resistant trail that they can later treat as a kind of native audit log, even though no single institution controls it.

Each standard crypto transaction moves value between alphanumeric addresses and writes that movement into the ledger with a permanent identifier that anyone can read.[13]

---

[11] Income-tax Act, No. 43 of 1961, § 2(47A) (India).
[12] Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction 77–90 (Princeton Univ. Press 2016).
[13] David Mills et al., Distributed Ledger Technology in Payments, Clearing, and Settlement, Fed. Rsrv. Fin. & Econ. Discussion Series No. 2016-095, at 10–15 (2016), https://doi.org/10.17016/FEDS.2016.095 (last visited Feb. 14, 2026).

Over time, these records form large transaction graphs in which investigators can follow flows of coins or tokens across hundreds of hops and many years.[14] For unspent-transaction-output systems like Bitcoin, every unit of value carries a visible ancestry of inputs and outputs; for account-based systems like Ethereum, changes in balances still leave a full public history for every account, so on-chain activity never really disappears.

This high transparency does not mean genuine anonymity. Users appear on the ledger as addresses, not names, so the system offers pseudonymity rather than full secrecy.[15] Once an exchange, broker or other virtual asset service provider links an address with a verified customer under KYC norms, that mapping can anchor later investigative work across the chain. The global anti-money-laundering framework now explicitly recognises that virtual assets are "digital representations of value" that move in pseudonymous form yet remain traceable with the right tools and data.

Blockchain forensics uses this structure to cluster addresses, label services and detect patterns that point toward particular actors.[16] Heuristics such as common-input ownership, change-address detection, or peel chains allow analysts to group multiple addresses as belonging to one wallet or entity, which then supports more targeted tax and AML inquiries. Europol and other enforcement bodies report successful asset seizures and criminal prosecutions where investigators followed such analytical leads across the ledger and finally linked them to exchange accounts or fiat cash-out points.[17]

---

[14] David Mills et al., Distributed Ledger Technology in Payments, Clearing, and Settlement, Fed. Rsrv. Fin. & Econ. Discussion Series No. 2016-095, at 10–15 (2016), https://doi.org/10.17016/FEDS.2016.095 (last visited Feb. 14, 2026).

[15] FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers 13–18 (2021), https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf (last visited Feb. 14, 2026).

[16] Michael Fröwis & Rainer Böhme, In Bitcoin We Trust? Allocation of Trust in Bitcoin and the Blockchain, 34 Digital Investigation 1, 3–7 (2020), https://doi.org/10.1016/j.diin.2020.300926 (last visited Feb. 14, 2026).

[17] Europol, Cryptocurrencies: Tracing the Evolution of Criminal Finances 8–12 (2021), https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf (last visited Feb. 14, 2026).

C. Artificial Intelligence, Machine Learning and Data Mining in Financial Regulation

Artificial intelligence in financial regulation works mainly through models that learn patterns from historic datasets and then flag behaviour that departs from those patterns in real time. Supervisors and tax administrations use supervised learning to classify transactions as low or high risk, and they use unsupervised techniques such as clustering or anomaly detection to surface new and unknown risk typologies.[18] In this way AI systems move beyond fixed rule engines, and they adapt as new fraud, evasion or laundering strategies appear in markets.

Machine learning systems in compliance environments typically draw on large volumes of structured and unstructured data. They ingest payment records, securities trades, exchange order books, KYC profiles, adverse media and now also blockchain transactions and wallet metadata.[19] Data mining methods then identify links across accounts, institutions and jurisdictions that human auditors would miss, for example repeated use of common devices, IP ranges or on chain addresses across ostensibly unrelated customers. For crypto tax enforcement this ability to fuse chain graphs with off chain customer data becomes central.

Regulators and international standards already encourage the cautious use of AI in financial supervision. The Financial Stability Board notes that machine learning can improve credit risk modelling, market surveillance and anti-money laundering monitoring, while warning about model risk and opacity.[20] The European Banking Authority also describes "RegTech" and "SupTech" applications where algorithms support supervisory review, thematic inspections and stress testing across large

[18] I. Glenn Cohen et al., The Impact of Artificial Intelligence on Financial Regulation, in Cambridge Handbook of Artificial Intelligence and the Law 245, 248–51 (Woodrow Barfield ed., 2024).
[19] Basel Comm. on Banking Supervision, Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors 24–27 (2018), https://www.bis.org/bcbs/publ/d431.pdf (last visited Feb. 14, 2026).
[20] Fin. Stability Bd., Artificial Intelligence and Machine Learning in Financial Services 2–6 (2017), https://www.fsb.org/wp-content/uploads/P011117.pdf (last visited Feb. 14, 2026).

regulated populations.[21] These discussions indirectly inform Indian agencies because they frame AI not as a luxury add on but as a necessary response to data intensive financial markets.

D. Blockchain Analytics and Crypto Forensics – Key Concepts, Techniques and Tools

Blockchain analytics builds structured intelligence on top of raw ledger data so that regulators, tax authorities and investigators can follow flows, identify actors and quantify risk. It treats each transaction as an edge and each address as a node, then constructs large transaction graphs on which algorithms can measure centrality, clustering and flow patterns.[22] These graphs reveal hubs such as exchanges, mixers, darknet markets or high-risk services and they show how crypto assets move between them over time.

Crypto forensics adds an evidentiary lens to this analytical work. It aims to preserve the integrity of collected data, document the acquisition process and generate outputs that courts can understand and rely upon.[23] Investigators typically begin by extracting blocks and transactions from full nodes or trusted data providers. They then normalise the information into forensic datasets, keep hash values for verification, and maintain clear chain-of-custody records for later legal proceedings. For tax enforcement, the same discipline is needed, because assessments and penalties may rest on reconstructed trading histories.

A key technique in blockchain analytics is address clustering. Analysts use heuristics such as common-input ownership, change-address patterns and co-spend behaviour to

[21] Eur. Banking Auth., EBA Report on Big Data and Advanced Analytics 19–25 (2020), https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2020/EBA%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics/882418/EBA%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf (last visited Feb. 14, 2026).
[22] Dirk A. Zetzsche et al., The "Dark Side" of Blockchain: Distributed Ledger Technology and the Rise of Anonymous Capital, 50 J. Corp. L. 95, 107–10 (2024).
[23] Sean Foley & Jonathan R. Karlsen, Forensic Methods for Cryptocurrency Investigations, 41 Comput. L. & Sec. Rev. 1, 3–7 (2025), https://doi.org/10.1016/j.clsr.2025.105987 (last visited Feb. 14, 2026).

infer that a group of addresses belong to one entity or wallet.[24] When they overlay this with attribution data from exchanges, seized databases, open-source intelligence and KYC records, they can label clusters as belonging to specific service providers or even identified individuals. This labelled graph then supports queries like whether a taxpayer's wallets interacted with high-risk services, or whether large unrealised holdings exist in unreported addresses.

E. Distinction between on chain, Off chain and Cross chain Data for Tax Risk Analysis

On chain data covers all information that a public blockchain stores in its blocks, such as addresses, transaction amounts, timestamps, smart contract calls and token transfers.[25] This data is transparent, globally replicated and in principle permanent, so tax authorities and analytics tools can read it without any cooperation from intermediaries. For crypto tax risk analysis, on chain data helps reconstruct trading activity, wallet balances, flows to exchanges and interactions with high-risk services, even when a taxpayer stays silent in their return.

Off-chain data sits outside the blockchain but relates closely to on chain events. It includes KYC records of exchanges, bank statements, trade confirmations, IP logs, device fingerprints and even chat records on trading platforms. Financial institutions and virtual asset service providers hold much of this material under customer-due-diligence rules, and they must retain it for AML and tax purposes.[26] Without off-chain data, on chain traces remain pseudonymous strings. Once investigators link an address cluster with a

[24] Sarah Meiklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, in Proceedings of the 2013 Internet Measurement Conference 127, 132–37 (ACM 2013), https://doi.org/10.1145/2504730.2504747 (last visited Feb. 14, 2026).
[25] David Mills et al., Distributed Ledger Technology in Payments, Clearing, and Settlement, Fed. Rsrv. Fin. & Econ. Discussion Series No. 2016-095, at 10–14 (2016), https://doi.org/10.17016/FEDS.2016.095 (last visited Feb. 14, 2026).
[26] Basel Comm. on Banking Supervision, Sound Management of Risks Related to Money Laundering and Financing of Terrorism 13–18 (2021), https://www.bis.org/bcbs/publ/d505.pdf (last visited Feb. 14, 2026).

verified customer file, the ledger becomes a detailed behavioural map that can reveal unreported gains and concealed holdings.

Cross chain data captures movements of value between different blockchains through bridges, wrapping mechanisms, atomic swaps and multi-chain protocols. Users increasingly move tokens from one chain to another to chase yields, reduce fees or obscure their history, and these movements often sit at the heart of sophisticated evasion or laundering schemes.[27] Analytics systems therefore need information about bridge contracts, locking and minting events, and swap transactions across several chains to follow the economic trail of a single position.

V. LEGAL FRAMEWORK ON CRYPTO TAXATION AND TRANSPARENCY IN INDIA

A. Statutory Treatment of Virtual Digital Assets under the Income tax Act 1961

Section 2(47A) of the Income Tax Act 1961 creates the foundational legal category of "virtual digital asset" and defines it broadly as any information, code, number or token, other than Indian or foreign currency, that represents value and can be transferred, stored or traded electronically.[28] The clause expressly includes non-fungible tokens and other notified digital assets, while also empowering the Central Government to exclude specified assets, so the definition can stretch with new token structures without frequent primary amendments.

The Finance Act 2022 introduces section 115BBH as a special charging provision for income from the transfer of any virtual digital asset, taxable at a flat rate of thirty per cent.[29] The rate applies whether the VDA would otherwise fall under capital gains or business income heads, and it operates as a self-contained regime that sits outside the

[27] Lennart Ante, Cross-Chain Bridges and DeFi: Risks, Opportunities and Analytics, 18 J. Risk Fin. Manag. 211, 214–19 (2025), https://doi.org/10.3390/jrfm18040211 (last visited Feb. 14, 2026).
[28] Income-tax Act, No. 43 of 1961, § 2(47A) (India).
[29] Union Budget 2022–2023, Scheme for Taxation of Virtual Digital Assets, in Union Budget 2022–2023: Budget Highlights 32–33 (Gov't of India 2022), https://www.indiabudget.gov.in/doc/bh1.pdf (last visited Feb. 14, 2026).

ordinary slab structure for individuals and firms. Budget documents describe this as a "specific tax regime" for VDAs, signalling that Parliament wanted a bright-line treatment which would be easier to administer and harder to arbitrage.

Section 115BBH also ring-fences the tax base in a strict manner. Only the cost of acquisition is deductible; no other expenditure, allowance or set-off is allowed, and any loss from transfer of a VDA cannot be set off against income from another VDA or against any other head, nor can it be carried forward.[30] Scholarly commentary notes that this creates a gross-revenue-based taxation model where traders bear full downside on failed positions but still pay tax on successful exits, which in turn may motivate more aggressive attempts to conceal or offshore gains. For tax-risk analytics this asymmetry is important, because it makes under-reporting profitable wallets a rational, though unlawful, strategy for some taxpayers.

The statutory treatment of VDAs also interacts with the anti-abuse provision in section 56(2)(x), which taxes receipt of "property" without consideration or for inadequate consideration, above specified thresholds.[31] Finance Act 2022 amends the Explanation to this section so that VDAs form part of the "property" basket; consequently, gifts of crypto between persons, or transfers at undervalue, may trigger tax in the hands of the recipient based on fair market value rules. Central Board of Direct Taxes (CBDT) materials on VDA taxation explain that, in such cases, tax may arise even if the transferor books no gain, so AI-driven systems must track inbound flows as carefully as disposals when they estimate undisclosed income.[32]

[30] Income-tax Act, No. 43 of 1961, § 115BBH (2) (India). (Income Tax India)
[31] Income-tax Act, No. 43 of 1961, § 56(2)(x) Explanation (d) (India).
[32] ELP, Taxation of Incomes from Virtual Digital Assets 3–5 (2023), https://elplaw.in/wp-content/uploads/2023/10/Budget-Buzz-Virtual-Digital-Assets.pdf (last visited Feb. 14, 2026). (Economic Laws Practice)

B. Tax Deduction at Source on VDA Transactions – Section 194S and Compliance Architecture

Section 194S of the Income Tax Act 1961 creates a stand-alone withholding regime for virtual digital assets, by requiring any person responsible for paying consideration to a resident for transfer of a VDA to deduct tax at source at one per cent of such sum.[33] Deduction takes place at the earlier of credit or payment, so even book entries in favour of the seller can trigger the obligation. The provision applies in addition to the charging section 115BBH, and it does not depend on whether the underlying income is later returned as capital gains or as business profits.

The design of section 194S uses monetary thresholds to protect small users but still capture active traders. For "specified persons", broadly small individuals and HUFs with limited business or professional turnover, TDS applies only if the aggregate consideration for VDA transfers in a financial year exceeds fifty thousand rupees; for all other payers the threshold is ten thousand rupees.[34] CBDT guidance clarifies that this aggregation runs from 1 April of the relevant year, even though the provision itself came into force on 1 July 2022, so once a payer crosses the threshold all later credits or payments attract TDS.

The compliance architecture distinguishes peer-to-peer deals from trades routed through exchanges or brokers. In direct over-the-counter transactions the buyer, as the person paying consideration, must deduct and deposit TDS.[35] Where trades occur through an exchange, circulars allocate the obligation either to the exchange, to the broker, or to the buyer depending on whether consideration flows in cash, in kind or through netting, and they prevent duplicate deduction by payment gateways by treating them as facilitators only. When consideration is wholly or partly in kind, the guidelines insist that tax be

[33] Income-tax Act, No. 43 of 1961, § 194S (India).
[34] CBDT, Circular No. 13 of 2022, Guidelines for Removal of Difficulties under Section 194S of the Income-tax Act, 1961 (June 22, 2022).
[35] CBDT, Circular No. 14 of 2022, Guidelines for Removal of Difficulties under Section 194S of the Income-tax Act, 1961 (June 28, 2022).

deducted and paid before the asset is released, which effectively forces parties to fund TDS from other resources.

C. Characterization of Crypto Gains – Capital Gains, Business Income and Other Sources

Characterization of income from virtual digital assets sits formally within the Income Tax Act 1961 heads of income, yet section 115BBH now overrides the rate and deduction rules for most practical purposes.[36] Before Finance Act 2022, taxpayers and advisors debated whether frequent crypto trading created business income or capital gains, by applying classical tests such as volume, continuity, intention and organisational set-up that courts had evolved in share-trading disputes.[37] Those judicial principles still matter for issues like audit requirements, maintenance of books, and set-off of non-VDA losses, even though tax on the "transfer" of VDAs now falls into a self-contained charging provision.

Where a taxpayer holds VDAs as long-term investments, disposes of them infrequently and does not use systematic leverage or market-making strategies, the gains would ordinarily bear the character of capital gains, with period of holding determining whether the gain is short-term or long-term.[38] In contrast, high-frequency trading, market-making, algorithmic arbitrage or dealing in VDAs for clients tends to show an adventure in the nature of trade, so the surplus assumes the character of business income.[39] CBDT and professional literature stress that these tests apply case-by-case, because the Act does not create a bright-line rule for what counts as "investment" versus "stock-in-trade" in the crypto context.[40]

Section 115BBH now taxes income from the transfer of any VDA at thirty per cent regardless of whether it falls under "Capital gains" or "Profits and gains of business or

[36] Byomkesh Panda, Taxation of Virtual Assets 6–9 (Nat'l Acad. of Direct Taxes 2024).
[37] CIT v. H. Holck Larsen, (1986) 3 S.C.C. 544 (India).
[38] Vatsa Akanksha, Taxation of Virtual Digital Assets in India: A Critical Analysis, 1 J. Tax L. 130, 139–41 (2022), https://hpnlu.ac.in/PDF/4fac1ba0-3e12-4d34-bc27-173871d9d869.pdf (last visited Feb. 14, 2026).
[39] CIT v. Associated Indus. Dev. Co. (P) Ltd., (1971) 82 I.T.R. 586 (S.C.) (India).
[40] Shalini Nagar, Virtual Digital Assets under Direct Taxation, Chartered Sec'y, Apr. 2025, at 18, 22–24, https://www.icsi.edu/media/webmodules/CSJ/April-2025/12.pdf (last visited Feb. 14, 2026).

profession".[41] However, the underlying head still influences collateral consequences. If the activity qualifies as business, turnover thresholds for tax audit, presumptive taxation inapplicability, and reporting of speculative or non-speculative business all come into play. If the holding counts as a capital asset, reporting falls under Schedule CG and interacts with loss-set-off rules in a different way, even though VDA-specific losses cannot be set off or carried forward under section 115BBH (2). For AI-driven risk engines this distinction can signal the presence of organised trading operations that warrant deeper scrutiny.

D. Gift, Inheritance and Off market Transfers of Crypto Assets under section 56 and Related Provisions

Section 56(2)(x) of the Income Tax Act 1961 taxes receipts of money or "property" without consideration or for inadequate consideration, above a monetary threshold, under the head "Income from other sources". Virtual digital assets now fall inside this anti-avoidance net because Finance Act 2022 expanded the definition of "property" to include VDAs. The provision therefore covers gifts of crypto assets and many off-market transfers where consideration is low or structured only on paper.

CBDT's explanatory materials and circulars state that the legislative intent was to bring gifting of VDAs into the tax base in a symmetrical manner with shares, jewellery and other movable capital assets.[42] Where a person receives VDAs without consideration and the aggregate fair-market-value of such receipts during a year exceeds fifty thousand rupees, the whole FMV becomes taxable in the hands of the recipient, unless a specific exemption applies.[43] The same rule applies where VDAs are received for inadequate consideration and the shortfall above fifty thousand rupees is taxed as income. This

[41] Income-tax Act, No. 43 of 1961, § 115BBH (1) (India).
[42] CBDT, Circular No. 23 of 2022, Explanatory Notes to the Provisions of the Finance Act, 2022, ¶ 6.4 (Nov. 3, 2022).
[43] Byomkesh Panda, Taxation of Virtual Assets 18–19 (Nat'l Acad. of Direct Taxes 2024), https://nadt.gov.in/writereaddata/MenuContentImages/TAXATION%20OF%20VIRTUAL%20ASSETS638701452732833757.pdf (last visited Feb. 14, 2026).

makes crypto gifts to non-relatives or to opaque entities a direct tax event at the point of receipt.

Standard gift-tax exemptions continue to operate. The Income Tax Act excludes from section 56(2)(x) any property, including VDAs, received from "relatives" as defined, under a will or by inheritance, on the occasion of marriage, or from specified charitable institutions.[44] CBDT tutorials on gifts now expressly mention VDAs as part of the prescribed movable property basket and clarify that genuine succession or family arrangements involving crypto will not be taxed at the receipt stage.[45] For tax-risk analysis however, large inflows of VDAs claiming to be from relatives or family trusts still raise red flags, because the relationship and occasion tests can be misused as camouflage.

E. Indirect Tax and GST Treatment of Crypto Exchanges and Service Providers

Goods and Services Tax law in India does not yet create a bespoke category for virtual digital assets, so authorities apply the general framework for "goods" and "services" under the Central Goods and Services Tax Act 2017 and the Integrated Goods and Services Tax Act 2017.[46] Crypto exchanges and service providers therefore analyse their supplies as online intermediary, facilitation or financial services and they charge GST on their fees, commissions and spreads, while the underlying peer-to-peer transfer of a VDA between two non-registered persons currently sits outside any specific GST entry.[47]

Departmental guidance and advance-ruling trends tend to treat platform fees, brokerage and wallet services as taxable supplies of services, usually at the standard eighteen per cent rate, because they amount to facilitation of trade in intangible assets.[48] Where an

[44] Vatsa Akanksha, Taxation of Virtual Digital Assets in India: A Critical Analysis, 1 J. Tax L. 130, 143–45 (2022), https://hpnlu.ac.in/PDF/4fac1ba0-3e12-4d34-bc27-173871d9d869.pdf (last visited Feb. 14, 2026).
[45] Income Tax Dep't, Tax Treatment of Gifts Received by an Individual or HUF 3–5 (2025), https://incometaxindia.gov.in/Tutorials/18.%20Tax%20treatment%20of%20gifts.pdf (last visited Feb. 14, 2026).
[46] Cent. Goods & Servs. Tax Act, No. 12 of 2017, §§ 2(52), 2(102) (India).
[47] Nitya Tax Assocs., Taxation of Virtual Digital Assets 13–16 (2023).
[48] Deloitte, Virtual Digital Assets – Key GST Issues 4–6 (2023).

Indian exchange provides services to non-resident customers, classification as export of services under section 2(6) of the IGST Act depends on place-of-supply rules and the location of the recipient, so many platforms must register in multiple States and apply complex apportionment of output GST on cross-border order books.[49] This complexity affects tax-risk analytics because mismatches between reported GST turnover and VDA volumes on-chain can signal hidden fee income or unregistered activity.

VI. INTERNATIONAL STANDARDS AND COMPARATIVE REGULATORY DEVELOPMENTS

Global tax and AML standards now treat crypto assets as a mainstream risk class and expect authorities to use advanced analytics for supervision and enforcement. The OECD's Crypto-Asset Reporting Framework (CARF) builds an automatic exchange regime for crypto data, similar to the Common Reporting Standard for financial accounts, and it defines a detailed set of data elements that reporting intermediaries must collect on customers, transactions and valuations.[50] CARF explicitly recognises that administrations will receive very large volumes of granular records and encourages the use of automated risk-analysis tools, including data-mining and machine-learning systems, to identify high-risk taxpayers in that stream.

The European Union has moved toward a comprehensive regime that joins market conduct, prudential control and tax transparency. Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) sets authorisation, governance, white-paper and reserve requirements for issuers and service providers, and it also mandates robust systems for AML compliance and transaction monitoring.[51] In parallel, the eighth amendment to the Directive on Administrative Cooperation (DAC8) extends mandatory reporting and

[49] Integrated Goods & Servs. Tax Act, No. 13 of 2017, § 2(6), §§ 12–13 (India).
[50] OECD, International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting Standard 11–14 (2023), https://doi.org/10.1787/896d79d1-en (last visited Feb. 14, 2026).
[51] Regulation 2023/1114, of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, 2023 O.J. (L 150) 40.

automatic exchange to crypto-asset service providers operating in or serving the EU, aligning EU law tightly with CARF and explicitly targeting evasion risks linked to offshore or cross-border exchanges.[52]

International AML standards mirror this trajectory. The Financial Action Task Force revised Recommendation 15 and its guidance to cover "virtual assets" and "virtual asset service providers", and it insists that VASPs must conduct customer due diligence, monitor transactions and implement the "travel rule" for originator and beneficiary information when they move funds.[53] FATF also stresses that supervisors and FIUs should make greater use of data analytics, artificial intelligence and blockchain-forensics techniques when they assess compliance and investigate complex crypto-related laundering patterns. For India, which is a FATF member, these texts act as a normative anchor for both PMLA amendments and the emerging use of blockchain analytics in enforcement.

VII. TYPOLOGIES AND MODES OF CRYPTO TAX EVASION

Non-reporting and under-reporting of gains remain the most basic typology. Many taxpayers simply omit virtual digital asset activity from their returns, or they disclose only a small subset of profitable trades while ignoring other wallets and exchanges.[54] Empirical work by international bodies records substantial gaps between survey-based ownership estimates and numbers of taxpayers who declare crypto income, which suggests systematic non-compliance rather than mere confusion.[55] In the Indian context, the high flat rate under section 115BBH and the ring-fencing of losses make such

[52] Council Directive 2023/2226, of 17 Oct. 2023 Amending Directive 2011/16/EU on Administrative Cooperation in the Field of Taxation (DAC8), 2023 O.J. (L 2023) 196.
[53] FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations 113–17 (Feb. 2023).
[54] Byomkesh Panda, Taxation of Virtual Assets 20–23 (Nat'l Acad. of Direct Taxes 2024).
[55] OECD, Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues 37–40 (2020), https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/10/taxing-virtual-currencies_e787d5db/e29bb804-en.pdf (last visited Feb. 14, 2026).

behaviour more tempting, because taxpayers bear tax on upside without relief for downside.

Misclassification of activity creates a subtler mode. Taxpayers may present organised high-frequency trading or market-making as casual investment, or they may book VDA receipts as loans, gifts or capital receipts to keep them outside business and professional income heads.[56] Some also attempt to understate fair-market-value at receipt for section 56(2)(x), especially for airdrops, staking rewards and off-market transfers. Professional commentary notes that these strategies exploit the information asymmetry between what is visible on chain and what is reported in books, which invites targeted use of analytics to reconcile the two.[57]

Use of foreign and unregulated platforms forms another typology. Individuals move funds from Indian bank accounts to offshore exchanges or peer-to-peer marketplaces, convert them into crypto, and then circulate assets through multiple wallets and chains before cashing out in another jurisdiction.[58] Chain-analysis reports show that a significant share of illicit and high-risk flows pass through a small number of offshore exchanges and cross-chain bridges, many with weak KYC.[59] For Indian tax authorities, such patterns create classic offshore-evasion risks, compounded by treaty and information-exchange challenges.

Privacy-enhancing technologies deepen opacity. Mixers, CoinJoin-type protocols, privacy coins and certain layer-two solutions aim to break straightforward transaction

[56] Vatsa Akanksha, Taxation of Virtual Digital Assets in India: A Critical Analysis, 1 J. Tax L. 130, 141–44 (2022), https://hpnlu.ac.in/PDF/4fac1ba0-3e12-4d34-bc27-173871d9d869.pdf (last visited Feb. 14, 2026).
[57] Shalini Nagar, Virtual Digital Assets under Direct Taxation, Chartered Sec'y, Apr. 2025, at 18, 24–26, https://www.icsi.edu/media/webmodules/CSJ/April-2025/12.pdf (last visited Feb. 14, 2026).
[58] OECD, International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting Standard 29–35 (2023), https://doi.org/10.1787/896d79d1-en (last visited Feb. 14, 2026).
[59] Chainalysis, The 2024 Crypto Crime Report 16–25 (2024), https://go.chainalysis.com/rs/503-FAP-074/images/2024-Crypto-Crime-Report.pdf (last visited Feb. 14, 2026).

graphs.[60] While the underlying chains may still be partially traceable, these tools make it much harder to link specific inflows and outflows, and they are often combined with "chain-hopping" across multiple networks.[61] FATF and Europol both document how criminals blend licit and illicit funds in such services, which complicates both AML and tax attribution of wallet balances.[62] Tax evaders can mirror these patterns to obscure the provenance of untaxed gains or to re-introduce assets as ostensibly clean capital.

VIII. LEGAL AND EVIDENTIARY DIMENSIONS OF USING AI AND ANALYTICS

A. Admissibility and Probative Value of Blockchain Forensic Evidence under the Bharatiya Sakshya Adhiniyam 2023

Blockchain traces and forensic reports qualify as "electronic records" under the Bharatiya Sakshya Adhiniyam 2023, because they consist of data, log files and derived visualisations stored in electronic form.[63] Sections dealing with electronic records recognise such material as "documents" and lay down special rules for proof of contents, so tax authorities and courts cannot treat blockchain screenshots or analytics dashboards as mere informal aids.[64] They must examine whether the party has satisfied the statutory conditions for admitting an electronic record in primary or secondary form.

The Adhiniyam continues the earlier policy that computer-output printouts or copies are admissible if specific technical conditions are met. Provisions analogous to former section 65B require proof that the computer was regularly used, that the data was fed in ordinary course, and that the output represents information derived from a properly functioning

[60] Michael Fröwis & Rainer Böhme, In Bitcoin We Trust? Allocation of Trust in Bitcoin and the Blockchain, 34 Digital Investigation 1, 6–8 (2020), https://doi.org/10.1016/j.diin.2020.300926 (last visited Feb. 14, 2026).
[61] Lennart Ante, Cross-Chain Bridges and DeFi: Risks, Opportunities and Analytics, 18 J. Risk Fin. Manag. 211, 214–19 (2025), https://doi.org/10.3390/jrfm18040211 (last visited Feb. 14, 2026).
[62] Europol, Decrypting the Criminal Use of Cryptocurrencies 22–27 (2023), https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Decrypting%20the%20Criminal%20Use%20of%20Cryptocurrencies.pdf (last visited Feb. 14, 2026).
[63] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 2(1)(e) (India).
[64] Id. §§ 61–65.

system.[65] For blockchain forensics this implies that investigators must demonstrate how they accessed the ledger, what software or nodes they relied on, how they exported transactions, and whether hash values or checksums verify that no later alteration occurred.[66] Certificates under these provisions therefore become central to the evidentiary status of analytics-generated graphs and tracing tables.

Probative value turns on reliability, completeness and explanation. Indian courts have emphasised in the context of other digital evidence that electronic records must be shown to be authentic and untampered and that expert testimony should explain the technology in a manner the court can test.[67] When tax or enforcement agencies place reliance on a blockchain-analytics report that clusters addresses or attributes a wallet to a taxpayer, they must lead evidence on the methodology, on error rates, and on the limitations of the heuristics used, rather than presenting the software output as an oracle. Comparative scholarship suggests that courts tend to admit such material, but they weigh it alongside corroborative financial records and admissions.[68]

B. Standards of Proof, Chain of Custody and Reliability of Algorithmically Generated Evidence

Standards of proof in crypto tax cases depend on the forum and consequence. Income-tax assessments and penalty proceedings follow the civil standard of preponderance of probabilities, and the Supreme Court in *CIT v. Durga Prasad More* and *Sumati Dayal v. CIT* permits authorities to rely on surrounding circumstances and "human probabilities" instead of accepting documents at face value.[69]Criminal prosecutions for wilful tax evasion, money-laundering or economic offences still require proof beyond reasonable

[65] Ratanlal & Dhirajlal, The Law of Evidence 1164–68 (Bharat Chugh ed., 28th ed. 2024).
[66] Vivek Dubey, Admissibility of Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023, 5 Indian J. L. & Tech. Pol'y 45, 57–60 (2024).
[67] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).
[68] Tatiana Cutts, Blockchains as Evidence, 17 Nw. J. Tech. & Intell. Prop. 1, 23–28 (2019), https://scholarlycommons.law.northwestern.edu/njtip/vol17/iss1/1 (last visited Feb. 14, 2026).
[69] Comm'r of Income-tax v. Durga Prasad More, (1971) 82 I.T.R. 540 (S.C.).

doubt, so algorithmically generated evidence cannot merely raise suspicion; it must support a coherent narrative that links wallets, transactions and intent.

The Bharatiya Sakshya Adhiniyam 2023 treats electronic and digital records, including blockchain extracts and AI-generated analytics output, as documentary evidence, and it elevates properly sourced electronic records from "proper custody" to the status of primary evidence.[70] At the same time, section 63 insists on a rigorous computer-output certificate which identifies the record, describes the manner of production, specifies devices used and affirms system integrity over the relevant period.[71] For blockchain analytics this translates into a formal chain of custody from node access or data-provider export, through parsing and enrichment, to the final tables, graphs and reports that are put before a court or tax tribunal. Hashing and logging of intermediate datasets becomes central, not optional practice.

Scholars analysing the new evidence code point out that chain-of-custody documentation now has to capture not only physical media, but also the life-cycle of digital artefacts, including their migration across servers and forensic tools.[72] In the context of AI-driven blockchain analytics, this means recording software versions, configuration settings, model parameters and time-stamped logs of each run that generates a risk score or address-clustering diagram.[73] Any break in this digital audit trail gives defence counsel room to allege contamination, selective disclosure or ex post reconstruction of incriminating paths on the chain.

[70] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 57 (India).
[71] Id. § 63.
[72] Vikas Singh, Impact of E-Records as Evidence in the Judicial System under the Bharatiya Sakshya Adhiniyam 2023, Metall. & Mater. Eng. (2025), https://metall-mater-eng.com/index.php/home/article/view/1383/762 (last visited Feb. 14, 2026).
[73] Electronic Evidence under Bharatiya Sakshya Adhiniyam – A Critical Analysis, Int'l J. Legal Liber. & Rsch. (2026), https://www.ijllr.com/post/electronic-evidence-under-bharatiya-sakshya-adhiniyam-a-critical-analysis (last visited Feb. 14, 2026).

C. Algorithmic Transparency, Explainability and the Right to Fair Hearing in Tax Proceedings

Use of AI and blockchain-analytics in tax administration must still respect the constitutional guarantee of fairness in State action. Indian courts derive a right to a fair procedure from Articles 14 and 21, and they insist that administrative decisions which affect rights cannot rest on undisclosed material or arbitrary criteria.[74] The Supreme Court's natural-justice jurisprudence emphasises that persons must know the case they have to meet and must have a meaningful opportunity to rebut adverse inferences.[75] When tax authorities rely on algorithmic risk scores or clustering outputs to select cases or frame assessments, these tools therefore become part of the "material" that must be open, at least in substance, to challenge.

Explainability sits at the heart of this obligation. If a VDA holder receives a notice based on an opaque model that labels her wallet "high-risk", but the authority refuses to disclose the underlying reasoning, the notice risks violating *audi alteram partem* because the assessee cannot understand or respond to the basis of suspicion.[76] Comparative scholarship warns against "black box" decision-making in public law and proposes a duty to give reasons that are intelligible to an ordinary person, even when the underlying model is complex.[77] In the tax context this may require authorities to share key factors, such as mismatch between reported income and on-chain flows, links to high-risk services, or patterns consistent with offshore-evasion schemes, while masking sensitive parameters or third-party data where strictly necessary.

Algorithmic transparency also links to reasoned-order requirements. Indian doctrine on administrative law insists that quasi-judicial authorities must record reasons that disclose

[74] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).
[75] Canara Bank v. Debasis Das, (2003) 4 S.C.C. 557 (India).
[76] Ujwala Uppaluri, Due Process and Automated Decision-Making in India, 15 Indian J. Const. L. 113, 124–28 (2024).
[77] Cary Coglianese & David Lehr, Transparency and Algorithmic Governance, 71 Admin. L. Rev. 1, 26–32 (2019), https://www.acus.gov/sites/default/files/documents/Coglianese%2520Transparency%2520and%2520Algorithmic%2520Governance.pdf (last visited Feb. 14, 2026).

a rational nexus between evidence and conclusions.[78] If assessing officers simply reproduce analytics outputs or boiler-plate language generated by decision-support systems, without independent evaluation, appellate forums may treat such orders as non-speaking and set them aside. Scholarly work on AI in governance therefore recommends that algorithms play an advisory role, while final decisions bear the stamp of human judgement, with clear articulation of why the officer accepted or rejected a particular model-based inference.[79]

D. Privacy and Data Protection Concerns – Interaction with the Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act 2023 treats tax authorities and VDA service providers as "Data Fiduciaries" whenever they process identifiable information such as PAN, bank details, KYC documents or wallet-attribution data. Processing for crypto tax enforcement usually relies on non-consensual grounds, namely performance of a legal obligation and exercise of a sovereign function, but the Act still requires purpose limitation, data-minimisation and reasonable security safeguards.[80] Consequently, large-scale ingestion of blockchain analytics, STR data and TDS trails into AI systems must remain demonstrably necessary and proportionate to the statutory mandate.

Policy analyses of the DPDP framework stress that even when the State processes personal data under "legitimate uses", it must give clear notices, define retention periods and enable core data-principal rights unless a specific exemption applies.[81] Guidance notes point out that criminal law, taxation and anti-money-laundering functions may attract tailored relaxations, yet they do not create a blanket immunity from privacy

[78] Mohinder Singh Gill v. Chief Election Comm'r, (1978) 1 S.C.C. 405 (India).
[79] Vidushi Marda, Artificial Intelligence and Public Decision-Making in India: A Framework for Accountability, Internet Democracy Project 18–23 (2022), https://internetdemocracy.in/reports/ai-public-decision-making-india-framework-accountability.pdf (last visited Feb. 14, 2026).
[80] Digital Personal Data Protection Act, No. 22 of 2023, §§ 2(5), 4, 7 (India).
[81] Mazars Advisory LLP, Digital Personal Data Protection Act 2023 – Key Features 3–6 (2023), https://ddtg.hp.gov.in/wp-content/uploads/2023/11/Mazars-Advisory-LLP.pdf (last visited Feb. 14, 2026).

duties.[82] For crypto tax analytics, this implies that internal governance documents should map each data flow – from VDA exchange KYC files to blockchain-forensics outputs – to a precise lawful basis and to a concrete retention and deletion schedule.

VDA service providers face a dual regulatory pull. On the one hand, PMLA and FIU directions require deep KYC, long-term record retention and active transaction monitoring; on the other hand, the DPDP regime requires them to avoid excessive collection, to secure data and to respond to access or correction requests from users.[83] Commentators on Indian crypto regulation note that exchanges must now design compliance programmes that reconcile these obligations, for example by role-based access controls, strong encryption and strict internal rules on secondary use of KYC and transaction data for marketing or profiling.[84] When tax authorities demand bulk data for analytics, they must also respect DPDP rules on data sharing between fiduciaries and on logging of such disclosures.

E. Constitutional Scrutiny – Proportionality, Non arbitrariness and Right to Privacy in AI driven Tax Surveillance

Constitutional review of AI-driven tax surveillance begins with the recognition that informational privacy forms an intrinsic part of Article 21, as affirmed by the nine-judge bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India*. The Court's later decision in *Puttaswamy (Aadhaar)* adopts a structured proportionality test: any rights-restricting measure must rest on valid law, pursue a legitimate State aim, be necessary in the sense of having no less restrictive alternative, and remain proportionate stricto sensu.[85] Academic commentary on these judgments stresses that digital-era surveillance schemes

[82] PRS Legislative Rsch., The Digital Personal Data Protection Act, 2023: Key Provisions and Issues 4–7 (2023), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited Feb. 14, 2026).
[83] CyberPeace Found., AML-CFT in Action: How Regulations Impact Virtual Digital Asset Service Providers (2024), https://www.cyberpeace.org/resources/blogs/aml-cft-in-action-how-regulations-impact-virtual-digital-asset-service-providers (last visited Feb. 14, 2026).
[84] Metalegal, Charting the Course: Essential Considerations for Indian Crypto Startups Amidst Evolving Regulation (May 23, 2025), https://www.metalegal.in/post/charting-the-course-essential-considerations-for-indian-crypto-startups-amidst-evolving-regulation (last visited Feb. 14, 2026).
[85] Justice K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 S.C.C. 1 (India).

must be justified not only by their objectives but also by the depth, breadth and duration of data collection and profiling they authorise.[86]

AI-driven monitoring of virtual digital asset activity for tax purposes easily engages this proportionality inquiry. The aim of curbing serious evasion and protecting the tax base qualifies as legitimate, but wide-ranging ingestion of TDS trails, VDA-exchange KYC files, financial intelligence reports and blockchain-analytics outputs into centralised risk engines must still satisfy necessity and balancing.[87] If the same enforcement outcomes can be achieved through more targeted queries, tighter sampling or narrower risk models, blanket continuous surveillance of all crypto users may appear overbroad. Scholarship on the Digital Personal Data Protection Act 2023 underlines that even when the State processes data under a statutory mandate, it must adopt data-minimisation and purpose-limitation practices consistent with Puttaswamy-style proportionality.[88]

Article 14 non-arbitrariness adds a second axis of scrutiny. Passive or active surveillance that relies on opaque scoring systems, undisclosed variables or biased training data risks producing unequal treatment between similarly situated taxpayers without a rational basis.[89] Analyses of AI in public decision-making warn that unexamined models can embed structural discrimination and can disproportionately flag certain demographic or behavioural profiles as "high-risk".[90] In tax enforcement, this would offend both equality and fairness, because persons could face intrusive searches, deep audits or reputational harm on the basis of patterns they cannot see or contest, while others escape scrutiny due to model blind spots.

---

[86] Priyanka Panigrahi & Aditi Mehta, The Impact of the Puttaswamy Judgement on Surveillance Jurisprudence in India, 15 NUJS L. Rev. 1, 10–15 (2022).
[87] Abhishek Padmanabhan, The Aadhaar Verdict and the Surveillance Challenge, 15 Indian J. L. & Tech. 1, 30–34 (2019).
[88] Srinivas Katkuri, A Critical Analysis of the Digital Personal Data Protection Act, 2023, 11 Int'l J. L. 22, 23–24 (2025), https://www.lawjournals.org/assets/archives/2025/vol11issue10/11235.pdf (last visited Feb. 14, 2026).
[89] Nupur Chowdhury, Privacy and Citizenship in India: Exploring Constitutional Morality and Data Privacy, 11 NUJS L. Rev. 483, 506–10 (2019).
[90] India Int'l J. Creative Res. Thoughts, AI and Constitutional Law: Freedom of Speech, Privacy and Equality 12–15 (Aug. 2025), https://ijcrt.org/papers/IJCRT2508728.pdf (last visited Feb. 14, 2026).

IX. FINDINGS AND CONCLUSION

The statutory architecture for virtual digital assets in India now rests on a coherent but deliberately stringent tripod of provisions: the definitional move in section 2(47A), the special charging rule and ring-fencing in section 115BBH, and the widened gift and off-market receipt rule in section 56(2)(x).[91] Together with section 194S TDS and the extension of PMLA to VDA service providers, the regime signals a policy choice in favour of granular third-party reporting and data-driven enforcement rather than voluntary self-declaration alone.[92] This design, while rational from a revenue-protection perspective, structurally increases incentives for sophisticated evasion that exploits cross-chain mobility, foreign platforms and pseudo-anonymity.

International standards now converge around the same data-intensive philosophy. The OECD's Crypto-Asset Reporting Framework and the EU's DAC8 regime both require detailed, machine-readable reporting from intermediaries, and they explicitly anticipate that tax administrations will employ advanced analytics and AI to cope with volume and complexity.[93] FATF guidance on virtual assets and on new technologies urges financial-intelligence units to combine traditional suspicious-transaction reporting with blockchain analytics and machine-learning tools.[94] Indian reforms on VDA taxation, PMLA coverage and DPDP obligations largely track these global trajectories, but institutional capacity and technical infrastructure still lag behind the ambitions of the legal texts.

The study shows that AI-assisted blockchain analytics can map a wide range of crypto-evasion typologies: simple non-reporting, misclassification of receipts, offshore routing,

[91] Byomkesh Panda, Taxation of Virtual Assets 6–10 (Nat'l Acad. of Direct Taxes 2024).
[92] CBDT, Circular No. 13 of 2022, Guidelines for Removal of Difficulties under Section 194S of the Income-tax Act, 1961 (June 22, 2022).
[93] OECD, International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting Standard 11–14, 29–35 (2023), https://doi.org/10.1787/896d79d1-en (last visited Feb. 14, 2026).
[94] FATF, Opportunities and Challenges of New Technologies for AML/CFT 26–31 (2021), https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf (last visited Feb. 14, 2026).

privacy-enhancing tools, circular trading and under-valued intra-group transfers.[95] When on-chain traces are linked with TDS data, GST returns, FIU reports and cross-border information exchanges, machine-learning models can flag anomalous wallets, reconstruct undeclared trading histories and estimate revenue at risk with a degree of precision that manual methods cannot match.[96] At the same time, the quality and legality of these outputs depend heavily on data governance, model validation, documentation of forensic workflows and the ability to explain risk scores in human-understandable terms.

Constitutional and evidentiary constraints therefore form an essential counterweight. The Bharatiya Sakshya Adhiniyam 2023 demands robust proof of integrity and proper custody for electronic evidence, while the Puttaswamy line of decisions requires that any AI-driven tax surveillance comply with legality, proportionality and non-arbitrariness under Articles 14 and 21.[97] The Digital Personal Data Protection Act 2023 overlays further duties of purpose limitation, minimisation and security, even when the State relies on sovereign-function grounds for processing.[98] Indian tax and regulatory agencies will thus need to build not only technical tools and specialist teams, but also transparent internal policies, audit trails and external accountability mechanisms, so that the deployment of AI and blockchain analytics against crypto tax evasion strengthens, rather than erodes, the legitimacy of the fiscal and enforcement state.

[95] Chainalysis, The 2024 Crypto Crime Report 16–25, 30–34 (2024), https://go.chainalysis.com/rs/503-FAP-074/images/2024-Crypto-Crime-Report.pdf (last visited Feb. 14, 2026).
[96] OECD Forum on Tax Admin., Tax Administration 3.0: The Digital Transformation of Tax Administration 35–41 (2020), https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/tax-administration-3-0-the-digital-transformation-of-tax-administration.pdf (last visited Feb. 14, 2026).
[97] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India); Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 57, 63 (India).
[98] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4, 7, 8 (India); PRS Legislative Rsch., The Digital Personal Data Protection Act, 2023: Key Provisions and Issues 4–7 (2023).

X. BIBLIOGRAPHY

A. Primary Sources (Statutes and Legal Instruments)

1. The Income Tax Act, 1961 (as amended by the Finance Act, 2022 introducing provisions on Virtual Digital Assets).
2. The Prevention of Money Laundering Act, 2002 and allied Rules and Notifications relating to Virtual Asset Service Providers.
3. The Digital Personal Data Protection Act, 2023.
4. The Bharatiya Sakshya Adhiniyam, 2023.
5. The Central Goods and Services Tax Act, 2017 and the Integrated Goods and Services Tax Act, 2017.
6. CBDT Circulars and Notifications relating to taxation of Virtual Digital Assets and TDS under Section 194S.
7. Financial Intelligence Unit–India (FIU-IND) Directions on reporting obligations for Virtual Asset Service Providers.

B. International Legal and Regulatory Instruments

1. OECD, *Crypto-Asset Reporting Framework (CARF)*, Organisation for Economic Co-operation and Development, 2022.
2. Financial Action Task Force (FATF), *Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2021.
3. Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA).
4. European Union Directive on Administrative Cooperation (DAC8) relating to crypto-asset reporting.

C. Judicial Decisions

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

2. *K.S. Puttaswamy v. Union of India (Aadhaar Case)*, (2019) 1 SCC 1.
3. *CIT v. Durga Prasad More*, (1971) 82 ITR 540 (SC).
4. *Sumati Dayal v. CIT*, (1995) 214 ITR 801 (SC).

D. Books and Commentaries

1. Taxmann, *Law and Practice of Income Tax*, Latest Edition.
2. V. Niranjan, *Digital Evidence and Cyber Law in India*, Eastern Book Company.
3. Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, O'Reilly Media.
4. Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press.

E. Reports, Articles, and Policy Papers

1. Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services*, 2017.
2. Europol, *Cryptocurrencies: Tracing the Evolution of Criminal Finances*, Latest Edition.
3. Chainalysis, *Crypto Crime Report*, Annual Reports.
4. RBI and Government of India policy papers on cryptocurrency regulation and taxation.