Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The Impact of Emerging Technologies on Business Laws: The Changing Regulatory Framework of E-Commerce

Krishna Kumar Yadav[a] Vinay Kumar Yadav[b]

[a]Assistant Professor, City Academy Law College, Chinhat, Lucknow, India [b]Assistant Professor, City Law College, Jankipuram, Lucknow, India

Received 07 May 2025; *Accepted* 09 June 2025; *Published* 12 June 2025

The rapid-fire elaboration of emerging technologies such as Artificial Intelligence(AI), blockchain, big data analytics, and the Internet of Things has revolutionised the geography of e-commerce and business law. This paper undertakes a comprehensive legal analysis of the shifting nonsupervisory paradigm in digital commerce, focusing on challenges surrounding consumer protection, data sequestration, algorithmic manipulation, central liability, antitrust enterprises, digital taxation, and online dispute resolution. It critically examines global and Indian legal developments, including the GDPR, India's Digital Personal Data Protection Act, 2023, FTC enforcement conduct, Competition Commission of India (CCI) cases, and WTO-led adjustment sweats. The study also explores the role of AI and blockchain in dispute resolution and translucency, probing into legal complications such as algorithmic conspiracy, gig frugality taxation, and the legal treatment of cryptocurrencies. With technology fleetly outpacing law, this paper argues for a future- evidence, encyclopedically harmonised legal framework that balances invention with moral rights, fairness, and responsibility in the digital frugality. Through an interdisciplinary approach, it proposes intertwined results to ground nonsupervisory gaps and promote independent growth in the e-commerce sector.

Keywords: *business, law, gdpr, e-commerce.*

INTRODUCTION

The rapid burst of emerging technologies has led to a paradigmatic shift in global trade, requiring an urgent and discerning legal system. Game-changing technologies such as artificial intelligence (AI), blockchain, immense data analytics, and the Internet of Things (IoT) have transformed transactional environments, business scalability, and consumer experience. However, the aforementioned breakthroughs also throw enormous regulatory conundrums, particularly about consumer protection, competition law, intermediary liability, and digital taxation.

The incessant evolution of e-commerce jurisprudence necessitates the delicate tension between technological dynamism and stability in rules. Governments and regulatory authorities across the world are dealing with novel questions of law emerging out of digital business models, e.g., data sovereignty, transnational liability, and platform regulation. Because legislation trails technologies, courts have been squarely tasked with implementing current statutes to help solve newly arisen questions of law conflicts.

This paper gives a critical examination of the dynamic legal environment of e-commerce regulation, critically evaluating contemporary regulatory challenges and possible jurisprudential development in statutory interpretation, judicial rulings, and international normative standards. It further examines the intersection among competition law, tax policy, and algorithmic fairness in shaping the parameters of electronic commerce in the future.

CONSUMER PROTECTION IN THE AGE OF THE INTERNET

We are living in the 21st century, and digital technology has revolutionised the world of business and consumer interaction beyond all recognition. From algorithmically filtered markets to AI-recommended products, the consumer journey has been more and more influenced by technologically black-boxed processes. While the process takes place at a speed never conceived before, it forms an intricate set of legal, ethical, and regulatory issues. The digital world, as convenient and as widely available as it now is, has also exposed consumers to new risks—anything from data misuse and algorithmic manipulation to imbalanced trade practices and an overall absence of serious responsibility on the part of big platforms. In such instances, the imperative for a strong consumer protection regime that dishes up realities about online commerce is not merely a desirable goal but a required one. Such a structure,

though, not only needs to fit in with conventional constructs of contract and tort law but also needs to adapt to encompass new issues such as platform liability, AI fairness, cross-border digital trade, and data sovereignty.

DATA PRIVACY AND CYBERSECURITY REGULATION

The most critical issue of digital consumer protection is protecting personal data. Each click, buy, and transaction leaves behind a trail of data, which is collected, stored, and demoralised, sometimes without the active consent of the individual. The increased pervasiveness of e-commerce websites, fintech apps, and social media sites has fueled apprehensions concerning data privacy and information security.

In the knowledge economy, personal data has become a currency traded, analysed, and exploited by corporations and also criminal elements. The vast scale of electronic commerce has necessitated stringent legal regulation over the assortment of personal data, necessitating a proper regulatory framework. Different countries have enacted inclusive Data Protection administrations, such as:

The European Union's General Data Protection Regulation (GDPR), 2018 (EU)[1], which was instigated in 2018, was an idealistic overreaction to these fears. The GDPR appreciates a human-centred data management method by mandating informed consent, minimisation of data, limitation of persistence, and a right to erasure (often referred to as the Right to be Forgotten).

It has also spurred similar legislation across more than 140 nations. This Advanced jurisdictive tool imposes severe responsibilities upon data controllers and processors, and it lays down principles of transparency, accountability, and voluntary consent. Jurisprudence of Google Spain SL v Agencia Española de Protección de Datos (2014)[2] in which the European Court of Justice (ECJ) promulgated the Right to be Forgotten. The Court ruled that Google, being a data controller, was duty-bound to remove superfluous or archaic information from its search results on a valid request from individuals. This decision emphasised that memory in cyberspace is not limitless and that people should have the ability to repossess their own stories in more permanent cyberspace. The decision flagged the idea of informational self-

[1] Data Protection Regulation 2016
[2] *Google Spain SL v Agencia Española de Protección de Datos* [2014] E.C.R. I-317

government and established a universal precedent for achieving a balance between freedom of expression and rights to secrecy.

The Digital Personal Data Protection Act 2023[3] is a sea-change in data confidentiality legislation. Heavily indebted to GDPR values enshrined, the Act contemplates a consent regime-based model of processing of personal data and introduces such bedrock principles as data fiduciaries, purpose limitation, and storage minimisation. It also suggests the institution of a Data Protection Board of India as an independent regulator for monitoring compliance, redressal, and adjudication. Non-compliance will attract a penalty of up to ₹250 crore, which is a strict direction in which India's digital consumer protection policy is moving.

This is especially relevant at a time when India is one of the world's prime digital economy markets with over 800 million internet users. Furthermore, the California Consumer Privacy Act (CCPA) 2020[4] establishes consumer rights to access, deletion, and opt-out, and the CCPA has had a substantial impact on global data privacy norms. Non-regulatory compliance brings forth significant financial penalties, as in the case of Facebook Ireland Ltd v Data Protection Commission (2021)[5], where the corporation was fined €265 million for security breaches in data. The extensive application of AI in consumer profiling is a demand for stringent encryption standards, transparency by algorithms, and breach notification practices as per law. Moreover, increasing anxieties surrounding deepfake technology and synthetic identity fraud also demand enhanced regulatory advancement in digital identity verification systems.

ALGORITHMIC MANIPULATION AND UNFAIR TRADE PRACTICES

As consumer experience increasingly becomes mediated by algorithms—whether for customised shopping, advertising, or product recommendation—new ethical and legal challenges have arisen. Algorithms as harmless as they seem can be coded to maximise gain at the expense of equity. Dark patterns, manipulative nudges, and misleading interfaces are some of the strategies applied in manipulating customer decisions without seeming awareness. Manipulations are extremely serious concerns concerning informed consent,

[3] Digital Personal Data Protection Act 2023
[4] California Privacy Rights Act of 2020
[5] *Facebook Ireland Ltd. v Data Protection Comm'n* [2021] IEHC 336 (H. Ct.) (Ir.)

consumer self-determination, and trading practices equity in the online space. AI-powered consumer targeting has caused immense concern about manipulative design strategies, false endorsement, and misleading advertising. Such exploitative trade practices have been addressed by the regulatory authorities by initiating remedial measures:

The Federal Trade Commission (FTC) Guidelines (USA)[6] have imposed significant penalties against participants with AI-assisted false advertising, such as in FTC v Fashion Nova, LLC (2022)[7]. It was the FTC's first case regarding efforts to conceal adverse customer reviews. Fashion Nova agreed to a settlement order that forbids the company from suppressing customer evaluations of its products. The firm was fined $4.2 million for the intentional suppression of negative consumer reviews. The FTC enforcement speaks to increasing awareness that technology has to be used ethically, and algorithms cannot be out of reach of conventional legal tools.

Consumer Protection (E-Commerce) Rules 2020[8], as part of the larger Consumer Protection Act 2019[9]. The rules insist on transparent advertisements, ban misleading presentations, and ask platforms to reveal the parameters for algorithmic ranking of products. Sellers must also give transparent terms of return policies, warranty terms, and price ingredients. In resolving platform neutrality, data openness, and algorithmic equity, the Rules are a significant advancement towards enabling ethical digital trade. With self-running AI-recommendation systems, pre-emptive regulatory action is necessary to neutralise algorithmic discrimination, manipulation of consumers, and price automation. In Case C-649/17 Amazon EU Sàrl v Verbraucherzentrale Baden-Württemberg, the Court of Justice of the European Union (CJEU)[10] reaffirmed that online marketplaces must ensure that algorithmic ranking and consumer profiling practices are transparent. The growing furore on AI content and intellectual property rights also makes international harmonisation in the regulation of AI's role in e-commerce more pressing.

[6] Federal Trade Commission Act 2022
[7] *Re Fashion Nova LLC* [2022] No. C-4759, Fed. Trade Comm'n
[8] Consumer Protection (E-Commerce) Rules 2020, s 3(i)
[9] The Consumer Protection Act 2019, s 1
[10] *Amazon EU Sàrl v Verbraucherzentrale Baden-Württemberg eV* [2019] ECLI:EU:C:2019:576 (CJEU 2019)

E-COMMERCE PLATFORM LIABILITY AND THE EMERGENCE OF ONLINE DISPUTE RESOLUTION (ODR)

Perhaps, the most contentious online consumer protection issue is e-commerce platform liability for goods and services sold through them. The legally traditional distinction between active sellers and passive intermediaries is increasingly anachronistic, as e-commerce platforms like Amazon, Flipkart, and Alibaba are no longer just online marketplaces. They control listings, determine rankings, provide logistics, and even provide financial services. Their more direct role has prompted a rethinking of intermediary immunity provisions.

The legal description of e-commerce platforms as passive intermediaries or active market participants remains a contentious issue in contemporary jurisprudence. Judicial decisions have increasingly considered platform liability for product defects and fraudulent transactions:

Oberdorf v Amazon.com Inc. 2019[11] (U.S. Court of Appeals, Third Circuit) relied on in holding that Amazon would be responsible for defective products of third-party sellers, effectively defying the conventional intermediary liability framework. The ruling upturned the long-established construction of intermediary immunity parallel to Section 230 of the U.S. Communications Decency Act.[12] Triggered a wider conversation about the role of online platforms in shielding customers. The advent of blockchain-integrated dispute resolution systems has also introduced an immutable evidentiary system, heightened the transparency of transactions and sped up dispute resolution. The incorporation of AI-enabled Online Dispute Resolution (ODR) mechanisms further raises legal efficiency by employing automated mediation and predictive legal analytics, as explained in the UNCITRAL Technical Notes on ODR (2016)[13].

AI-enhanced ODR also raises concerns about procedural fairness, prevention of bias, and comprehensibility of algorithmic decision-making in commercial disputes. Even in India, this transition is echoed in the Information Technology (Intermediary Guidelines and Digital

[11] *Oberdorf v Amazon.com Inc.* [2019] 930 F.3d 136
[12] Communications Decency Act 1996
[13] 'Technical Notes on Online Dispute Resolution' (*United Nations Commission On International Trade Law*, 30 May 2007) <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/v1700382_english_technical_notes_on_odr.pdf> accessed 02 May 2025

Media Ethics Code) Rules 2021[14], which impose graduated responsibility upon platforms according to their size and reach. These regulations provide for grievance redressal, transparency reporting, and obligations of due diligence. The upcoming Digital India Act will likely further specify these duties following the cue from the EU's Digital Services Act (DSA), 2022[15], that places stringent duties on very large online platforms in illegal content, systemic harm, and algorithmic responsibility areas.

ONLINE DISPUTE RESOLUTION (ODR): THE WAY FORWARD FOR CONSUMER REDRESSAL

As more transactions go online, there is a growing demand for cost-effective, scalable, and efficient resolution mechanisms. Conventional litigation is generally not well-placed to handle low-value, cross-border e-commerce disputes. ODR platforms have stepped into the situation as a disruptor. The UNCITRAL Technical Notes on ODR (2016)[16] is a global standard, promoting accessible, neutral, and secure systems. SAMA and CADRE have picked up pace in India, especially with COVID-19, for resolving commercial and landlord-tenant litigation using AI-driven mediation software. These platforms provide asynchronous communication, computer-based document management, and algorithmic matching of the mediators, hence improving efficiency and reducing backlog. As courts increasingly engage with ODR, its cooperative integration with conventional judicial systems is now imminent, particularly in light of the Digital India vision and ease of doing business initiatives.

ETHICAL AND LEGAL ENCOUNTERS IN AI-MEDIATED CONSUMER EXCHANGES

The arrangement of AI-based chatbots, virtual assistants, and sovereign decision-making systems in e-commerce poses challenging ethical and legal challenges, predominantly in the domains of misinformation, algorithmic bias, and vulnerability to AI-facilitated fraud. The EU AI Act (2021)[17] is one of the boldest efforts at AI regulation.

The Act differentiates between AI applications in terms of risk level—unacceptable for use are such things as social scoring, and subject to intense conditions are high-risk applications

[14] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
[15] Regulation (EU) 2022/2065of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC 2022
[16] *Ibid*
[17] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 2024

such as biometric identification, lending money, and hiring decisions. Transparency, human control, audit trails, and data governance are major requirements. To this, UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021)[18] is the first global normative instrument to articulate the principles of fairness, accountability, and explainability for artificial intelligence systems. Regulatory intervention has to ensure culpability in AI-mediated commercial interactions through structured oversight mechanisms, including:

Forced Algorithmic Audits: Forcing accountability within AI models of decision-making, just like the proposed EU Artificial Intelligence Act (2021).

Standards of Compliance of Ethical AI: Establishing global best practices in the responsible use of AI, just like UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021).

Jurisprudence – Loomis v Wisconsin (2016):[19] Addressed constitutional concerns posed by AI-powered risk assessment software in judicial adjudication, affirming the necessity of human intervention in algorithmic decision-making processes.

While the Court affirmed the application of COMPAS software, it did so with the additional insistence of human review and a warning against black box decision-making. This case is more significant than for criminal law because these types of tools are increasingly being used in financial services, insurance risk rating, and even e-commerce pricing—areas where unintelligible algorithms can result in discriminatory consumer outcomes.

Additional concerns come with AI-aided decision-making in credit scoring and financial transactions. Algorithmic bias has resulted in discriminatory lending, as evidenced by a number of regulatory investigations into the application of opaque credit-scoring techniques by fintech firms. Moreover, AI-generated content moderation policies present due process concerns, necessitating more open legal guidelines for addressing AI-driven content take-downs and platform responsibility requirements.

The legal climate governing e-commerce and emerging digital technologies is changing on a constant basis, calling for a sophisticated interaction between legislative action, judicial rulings, and regulatory steps. The courts, legislatures, and enforcement agencies worldwide

[18] 'Ethics of Artificial Intelligence – The Recommendation' (*UNESCO*, 2021) <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> accessed 02 May 2025
[19] *State v Loomis* [2016] 881 N.W.2d 749

are busy constructing a framework of law to harmonise technological innovation with the need for consumer protection, standards of competition law, and sustainable AI regulation. In the shadow of the irreversible expansion of e-commerce, future legal development must target an equilibrium between technological innovation and regulatory predictability.

Harmonisation of the regulatory frameworks across jurisdictions will be important in ensuring that the speed of technological innovation continues to be kept in step with fundamental principles of legal certainty and equitable consumer protection rights. The role of global organisations (e.g., United Nations Commission on International Trade Law or UNCITRAL and World Intellectual Property Organisation or WIPO) in regulating on a harmonised basis.

ANTITRUST AND FAIR COMPETITION IN THE DIGITAL MARKET

The digital economy has constructed platform monopolies that dominate end-to-end ecosystems—search, social media, retail, and cloud computing. Google, Amazon, and Facebook have been accused of mistreating dominance by engaging in predatory pricing, hustling, exclusive dealing, and self-preferencing. Such anti-competitive practices are not just detrimental to consumers but also suffocate innovation and limit market entry for entrants.

In United States v Microsoft Corp. (2001), the enclosure of Internet Explorer in the Windows operating system was an antitrust offence that established a precedent for regulating digital monopolies. In European Commission v Google (2017),[20] Google was penalised €2.42 billion by the EU for algorithmic manipulation of search outcomes to favour its contrast shopping service at the expense of competitors.

In India, the Competition Commission of India (CCI) has initiated various investigations against Amazon and Flipkart's conduct, specifically on their demand for preferential treatment of certain sellers, deep disbelieving strategies, and algorithmic ranking prejudice. Such investigations indicate a greater willingness of Indian regulators to venture into digital spaces and safeguard competition.

A New Frontier in Antitrust Law. As the algorithms are developed with AI technology, there arises a fear of increased implicit collusion by computers without any explicit coordination

[20] *Google LLC, formerly Google Inc. and Alphabet, Inc. v European Commission* [2021] Case T-612/17

by humans. In the case of UK Competition and Markets Authority v Trod Ltd. (2016),[21] two online retailers were penalised for applying algorithms to collude over prices on art posters, thus recording one of the first antitrust cases involving algorithmic collusion.

The OECD and academicians from institutions such as Harvard and MIT have pushed for AI audits, regulatory sandboxes, and source code disclosures to detect and prevent algorithmic collusion. As algorithms become more autonomous, these measures are intended to ensure accountability is based on human agency and competitive integrity in markets is safeguarded and not undermined using digital technologies.

FAIR TRADE PRACTICES AND COMPETITION LAW

Market Dominance and Anti-Competitive Conduct: The anticompetitive predispositions of powerful e-commerce conglomerates such as Amazon, Alibaba, and Flipkart raise profound antitrust concerns, necessitating more regulatory scrutiny. Performances such as predatory pricing, deep discounting, and delimited supply arrangements have drawn keen competition regulator focus around the world.

Regulators such as the Competition Commission of India (CCI), the European Commission, and the United States Federal Trade Commission (FTC) have sought to curtail digital market distortions by employing proactive enforcement. In addition, the role of AI-based pricing algorithms in facilitating tacit collusion and algorithmic coordination has been an emerging area of regulatory investigation.

Pivotal judgments such as United States v Microsoft Corp. (2001)[22] and European Commission v Google (2017)[23] exemplify the evolution of legal strategies used to battle market dominance and antitrust practices by digital companies. The contemporary regime of regulation continues to consider the monopolisation of data as a principal factor in classifying anti-competitive conduct, embracing the realisation that control of users' information creates a great competitive advantage for digital economies.

[21] *UK Competition and Markets Authority v Trod Ltd.* [2016] Case 50223
[22] *United States v Microsoft Corp.* [2001] 253 F.3d 34
[23] *Google LLC, formerly Google Inc. and Alphabet, Inc. v European Commission* [2021] Case T-612/17

ALGORITHMIC COLLUSION AND PRICE OPTIMIZATION CHALLENGES

The advent of AI-driven dynamic pricing algorithms has thrown unprecedented challenges to antitrust enforcement. While such systems promote market efficiencies, they inadvertently foster algorithmic collusion, where competing platforms collude on prices without express communication. Traditional competition laws, based on human decision-making paradigms, are ill-equipped to deal with the complexities of automated price manipulation. Accordingly, regulatory mechanisms must substantially shift to encompass requirements of algorithmic transparency and AI audit processes. The UK Competition & Markets Authority v Trod Ltd case of 2016[24] established that plans to fix prices using algorithms functioning automatically were susceptible to highly severe antitrust testing. Subsequent literature has further strengthened the need for fear of AI-driven price changes, conceivably causing unforeseen monopoly practices and necessitating anticipatory action on the part of regulatory bodies. As the ability of AI evolves, competition authorities must refine their methods of assessment so that they are able to determine and react to collusive tendencies that lie outside conventional legal paradigms of coordination.

EVOLVING REGULATORY DISTINCTIONS BETWEEN MARKETPLACE AND INVENTORY MODELS

The traditional separation between marketplace and inventory-based models of e-commerce is becoming ever more blurred and necessitates the rebalancing of existing paradigms in regulation. In jurisprudences such as that of India, foreign direct investment policies set limits on direct stock management by foreign e-commerce entities to guarantee competitive market equilibrium. However, the intensification of mixed business models has disempowered the effectiveness of such regulatory distinctions.

Notably, rumours such as Amazon's alleged favouritism of selected sellers, investigated by the Competition Commission of India, further heighten the need for a sophisticated approach. Regulators and courts must weigh consumer interests against economic freedom while avoiding marketplace platforms exploiting structural loopholes to avoid competition

[24] *UK Competition & Markets Auth. v Trod Ltd* [2016] Case 50223

law. The legal description of digital marketplaces as mere intermediaries is increasingly untenable, given their increasing influence on pricing, logistics, and consumer choice.

CROSS-BORDER DIGITAL TRADE AND REGULATORY HARMONIZATION

In more integrated times, commerce has departed from the traditional cross-border exchange of goods to frictionless, real-time digital commerce across physical borders. Digital commerce platforms such as Amazon, Alibaba, and Shopify sell in dozens of countries at the same time, enabling billions of consumers to engage in cross-border digital commerce. This record level of digital commerce, however, raises challenging questions of law regarding jurisdiction, regulatory arbitrage, enforcement of consumer protection, and extraterritorial application of domestic law. Legal harmonisation has emerged as a cutting-edge global issue due to challenges such as data localisation obligations, cross-border taxation obligations, and convergences of privacy law.

Against these encounters, the World Trade Organisation (WTO) launched the Joint Statement Initiative (JSI) on E-Commerce in 2019[25], involving around 76 member economies. The JSI seeks to carry a global rule system to regulate significant essentials of digital trade, including cross-border flows of data, data localisation, digital services taxation, and cooperation on cybersecurity.

The initiative seeks to deliver multilateral predictability by consolidating the scattered patchwork of digital trade rules already negotiated. Unwelcome opposition, however, has arisen from developing economies like India, which have expressed the fear that highly liberalised rules of digital trade would be a threat to national economic interests, compromise data sovereignty, and disproportionately end up in the hands of tech monopolies of the Global North.

India's opposition to WTO e-commerce negotiations, as reflected in its reluctance to commit to binding commitments on cross-border data flows and non-imposition of customs duties on electric transmissions, is the endpoint of a broad policy approach to protect domestic industries and provide a fillip to MSMEs. The Indian government has never believed that the free flow of digital trade, in the absence of corresponding regulatory protection, will lead to

[25] 'Joint Statement Initiative on E-commerce' (*World Trade Organisation)* <https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm> accessed 03 May 2025

an asymmetric gain for multinationals to the detriment of indigenous innovation and employment generation.

But yet another area where global harmonisation of law became unavoidable is taxation. The digital economy exposed the vulnerability of traditional tax systems based on physical presence and permanent establishment. Global technology giants like Meta, Alphabet (Google), and Amazon time and again make billions of dollars out of user bases in nations where they pay little or no tax. In this context, the Organisation for Economic Co-operation and Development (OECD)[26] launched the Base Erosion and Profit Shifting (BEPS)[27] initiative, culminating in Pillar One and Pillar Two proposals in 2021. Pillar One redistributes taxing rights to merchandise jurisdictions, in the sense that a portion of profits is taxed where users and consumers are, and not where they are located. Pillar Two suggests a 15% global minimum tax rate for businesses to end profit-shifting and tax avoidance arrangements.

These OECD guidelines are a key step toward global tax justice, but the problem of putting them into practice keeps them from reaching their goal. Sovereignty questions, administrative feasibility, and political consensus are still there to prevent their full enforcement around the world. They are, nonetheless, a benchmark for the establishment of a rules-based digital economy in which multinational digital behemoths are held accountable for their economic footprint in any market they venture into.

DIGITAL TAXATION: OPPORTUNITIES AND CHALLENGES

Global Tax Equity and Digital Services Taxes (DSTS): India's Equalisation Levy, introduced in 2016 and revised in 2020, is a tax on non-resident digital enterprises collecting revenues from Indian consumers with no physical presence in India. The step is to make Indian and foreign service providers tax-neutral. But unilateral digital levies have elicited strong criticism from the United States, which sees them as discriminatory against US technology companies.

The U.S. Trade Representative (USTR), following Section 301 of the Trade Act Initiated probes into India's Equalisation Levy and similar measures, threatening tariffs retaliation.

[26] *Ibid*
[27] 'Action Plan on Base Erosion and Profit Shifting' (*OECD*, 19 July 2013) <https://www.oecd.org/en/publications/action-plan-on-base-erosion-and-profit-shifting_9789264202719-en.html> accessed 03 May 2025

This increased tension warrants multilateral remedies such as the OECD's Global Tax Deal (2021)[28], signed by 138 nations, including India. The deal suggests sharing some digital tax receipts with market jurisdictions and a 15% global minimum tax for big multinational enterprises.

This proposal, if adopted, would end unilateral digital levies and the spectre of trade wars. It is also a change of paradigm from geography to a user-tax system, which is in link to the very nature of the digital economy. But this to occur would need comprehensive reforms in domestic tax legislations, multilateral treaty modifications, and advanced data-exchange facilities between tax administrations.

The globalisation of digital commerce has made it difficult to have traditional tax models, so new thinking in fiscal control is required. The Association for Economic Co-operation and Development (OECD) has suggested the implementation of a global minimum tax framework to counteract tax evasion by multinational digital companies.

India, France, and the UK have introduced Digital Services Taxes (DSTs) to tax revenue engendered by foreign e-commerce players in their jurisdictions. Extraterritorial application of DSTs has, however, created trade disputes and obligatory multilateral taxation collaboration to prevent double taxation and inconsistent regulatory environments. The ongoing negotiations under the OECD/G20 Inclusive Framework seek to reach a consensus-based solution to the digital tax matters. However, unilateral tax measures continue to fuel geopolitical tensions, which further create retaliatory trade policies that can hamper global e-commerce growth.

TAX IMPACTS OF THE GIG AND SHARING ECONOMY

The rising prevalence of gig work in the digital economy poses specific taxation difficulties. Uber, Airbnb, and Fiverr are some platforms whose business is conducted within decentralised labour relationships with a propensity towards avoiding conventional tax obligations.

Consequently, tax authorities need to create tax regimes that foster balanced revenue distribution with the protection of the rights of gig workers. Policy discourse, including the

[28] *Ibid*

European Commission's platform workers directive, emphasises the challenge of applying fair taxation without discouraging innovation. Taxation charges are dependent directly on gig workers' legal status as independent contractors or employees and necessitate accurate legislative intervention.

Labour Rights and Fiscal Responsibilities. Yet another new space for regulation over the internet is the gig economy, spearheaded by Uber, Ola, Zomato, Swiggy, and Urban Company. These platforms treat employees as independent contractors to avoid offering conventional employer benefits like health care, minimum wages, and social security. While the gig economy has promoted flexibility and employment, it has also created problems of insecure terms of employment, no bargaining, and uncertain tax liabilities.

With this, the European Union has implemented the Platform Work Directive (2022)[29], which attempts to consider gig workers as employees in some instances—i.e., when the platform dictates prices, has control over the job, or limits the worker's independence to decline assignments. Considering workers in this way would grant rights to workers under minimum wage, paid time off, and unemployment insurance, essentially harmonising platform work with mainstream labour law.

India has made a beginning in this direction through the Code on Social Security, 2020[30], which was notified in 2023. It proposes the setting up of Social Security Boards at the state and national levels to enroll and administer welfare benefits for gig and platform workers. Taxation and classification of work are still unclear. Welfare schemes are extended to gig workers in name, but no special tax regime for their income is proposed, and no platform companies are mandated to deposit equivalent amounts into provident funds or health insurance.

The absence of an effective regulatory framework for taxation of the gig economy and labour rights continues to yield an uneven playing field—one that significantly benefits gigantic platforms at the expense of ordinary employers and workers alike. Tax deductibility, GST

[29] 'Improving the working conditions of platform workers' (*Think Tank European Parliament*, 08 January 2025) <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)698923> accessed 03 May 2205
[30] The Code on Social Security 2020

liability, and portability of social security must be tackled by future reforms in a digitally native workforce.

CRYPTOCURRENCY TRANSACTIONS AND BLOCKCHAIN TAXATION

The advent of cryptocurrency-driven online transactions has necessitated an examination of tax compliance systems. Governments across the globe are struggling to categorise cryptocurrencies as taxable digital assets and deal with enforcement issues surrounding anonymity and decentralisation. A deployment of decentralised digital identity solutions can improve tax compliance and maintain consumer anonymity in blockchain-based transactions. Regulatory reforms, including the U.S. Internal Revenue Service (IRS)[31] Designation of cryptocurrencies as taxable property, mark the increased legal attention to blockchain-based economic transactions.

The US Internal Revenue Service (IRS) has classified cryptocurrencies as property and not as currency. Therefore, any exchange, sale, or disposal of crypto incurs a capital gains tax liability. Starting from 2022, the IRS required all taxpayers to report cryptocurrency assets and transactions on Form 1040, representing enhanced enforcement and monitoring. India's response also has been momentous.

The Union Budget 2022 announced a uniform 30% tax on all virtual digital assets' profits, no categorisation based on holding period, and a 1% Tax Deducted at Source (TDS) on each transfer.[32] Although the step, in an attempt to curb speculative trading and generate revenues, has also been criticised as being too draconian and ambiguous in terms of loss set-offs, staking income, airdrops, and NFTs, it is a trailblazer to bring the crypto economy within the formal tax net.

These trends suggest that any future regulatory frameworks for cryptocurrencies will need to strike a balance between investor protection and innovation. Suggested ideas have included cross-border data reporting standards, crypto-asset service provider licenses, and centralised registries, something that the Financial Action Task Force (FATF) and International Monetary Fund (IMF) already have on the table. In addition, the coupling of

---

[31] *Ibid*

[32] 'Memorandum Explaining the Provisions in the Finance Bill, 2022' (*Ministry of Finance*, 31 January 2022) <https://www.indiabudget.gov.in/budget2022-23/doc/memo.pdf> accessed 03 May 2025

smart contracts with tax enforcement is a potential future for the automation of compliance through self-enforcing fiscal obligations.

CONCLUSION

The Digital Age Road Ahead for Business Law. The digital economy is changing at a pace faster than the legal system can keep up with. Confronted with exponentially changing technologies such as AI, blockchain, quantum computing, and the metaverse, which are redefining human life, work, business, commerce, and governance, the legal system must change to keep up with these epochal changes.

The future of business law lies in the ability to internalise elements of innovation, consumer protection, and global cooperation and to adopt an integrated and future-proofed legal system. National legal systems must invest in infrastructure, e-courts, AI-assisted regulatory compliance software, and intra-agency coordination. International organisations such as the WTO, OECD, UNCITRAL, and WIPO must take the lead to reform binding cross-border data management, platform responsibility, digital taxation, and the responsible use of AI.

Regime convergence and decentralised enforcement mechanisms such as blockchain-based audits and regulation of smart contracts can usher in a new world of digital justice. In this boundaryless, dynamic new world, business law can no longer rest on territorial sovereignty. It must be a multidisciplinary, multilingual, modular system with constitutional values, private ordering, public accountability, and technological flexibility. Its eventual goal must be to produce a trust-based, equitable, and inclusive digital economy where innovation is feasible without undermining human rights, democratic control, and sustainable development.

With the expansion of electronic commerce, regulatory mechanisms need to evolve and confront challenges of market concentration, algorithmic collusion, and borderless tax evasion. Use of AI-friendly mechanisms, blockchain transparency, and harmonised legal standards will be instrumental in making the online market competitive and just. The jurisprudential discussion of new technologies and e-commerce calls for an interdisciplinary approach that combines legal principles with technological advancements in a bid to build robust regulatory solutions.