IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Data Protection in Modern Commerce: *Balancing Trust, Transparency, and Global Trade*

A Conceptual Analysis of Privacy, Regulation, and Commerce

Gurpreet Singh Kalsi
Assistant Professor
Department of Commerce
Babbar Akali Memorial Khalsa College Garhshankar (Hoshiarpur)
Punjab (India)

Abstract: Data protection has emerged as one of the defining commercial and regulatory challenges of the digital age. This paper examines how privacy governance shapes consumer trust, corporate transparency, and cross-border trade in modern e-commerce. Drawing on primary regulatory frameworks — including the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA/CPRA), and India's Digital Personal Data Protection Act (DPDP) — alongside empirical data from IBM, Cisco, Usercentrics, DLA Piper, and Surfshark, the paper analyses the financial, reputational, and operational consequences of data breaches and non-compliance. Key findings include: the global average breach cost of $4.44 million in 2025 (IBM); over €7.1 billion in cumulative GDPR fines since 2018; a data privacy market valued at $175.3 billion and growing at 16.8% annually; and evidence that 75% of consumers will not purchase from organisations they do not trust with their data. The paper further explores the emerging risk posed by ungoverned artificial intelligence adoption, including "shadow AI" practices that cost organisations an average of $4.63 million per breach. Strategic recommendations are provided for both organisations and individuals, covering governance frameworks, technical safeguards, third-party risk management, and consumer best practices. The analysis concludes that data protection is no longer merely a legal obligation but a measurable source of competitive advantage and a prerequisite for sustainable participation in global digital commerce.

Index Terms - data protection; e-commerce; consumer trust; GDPR; CCPA; data breaches; privacy regulation; cybersecurity; AI governance; digital trade; transparency; personal data; compliance; information security; shadow AI; third-party risk

1. INTRODUCTION

In the digital era, data protection in commerce has evolved from a technical requirement into a foundational pillar that underpins trust between buyers and sellers, demands radical transparency regarding data utilization, and dictates the rules of international trade. As e-commerce platforms increasingly rely on personal data — including identities, payment details, and behavioral profiles — weak protection measures directly undermine customer confidence and purchasing behavior.

The stakes could not be higher. According to IBM's 2025 Cost of a Data Breach Report, the global average cost of a data breach fell slightly from $4.88 million in 2024 to $4.44 million in 2025, largely due to faster AI-assisted detection. However, U.S. organizations bucked this trend, with breach costs rising 9% to a record $10.22 million. Meanwhile, cumulative GDPR fines have surpassed €7.1 billion

since 2018 — a 21% year-over-year increase — and in 2025 alone, over 330 fines totalling nearly €1.15 billion were issued across Europe.

The global data privacy market, valued at $175.3 billion in 2025, is projected to reach over $509 billion by 2032 — growing at a compound annual rate of 16.8%. This underscores the emergence of data protection not as a cost center, but as a core strategic investment. Robust data protection is now a basic market expectation and a genuine competitive differentiator.

2. The Three Pillars: Trust, Transparency, and Trade

Data protection functions as a commercial catalyst through three primary mechanisms that reinforce one another in ways now backed by extensive empirical evidence.

2.1 Trust

Consumer trust is increasingly quantifiable and financially significant. Research confirms that 75% of consumers will not purchase from organizations they do not trust with their personal data, and 60% say they would spend more money with a brand they trust to handle data responsibly. Conversely, a single data breach negatively affects purchase intent for 59% of consumers. IBM's 2025 report further underscores the commercial link: lost business — driven by customer churn and reputational damage — remains one of the largest cost components of any breach incident.

Trust is not evenly distributed across sectors. Finance and public institutions enjoy comparatively higher trust, while retail, automotive, and technology companies lag behind. Highly regulated industries appear to benefit from compliance signalling: consumers equate regulatory oversight with security diligence. For e-commerce, where trust must be established virtually, visible security controls, clear consent mechanisms, and responsive breach handling are decisive factors in purchase decisions. Research shows that consumers are willing to pay premium prices to merchants with demonstrably better privacy practices — a finding that quantifies privacy as a source of pricing power, not merely a compliance checkbox.

2.2 Transparency

Transparency has evolved from a vague aspiration into a measurable consumer expectation. A 2025 global study by Usercentrics surveying 10,000 consumers found that 77% do not fully understand how their data is handled, and 40% believe they have rights but don’t know what they are. This information deficit creates both a compliance risk and a strategic opportunity: brands that educate and empower users can convert confusion into loyalty.

Practically, transparency means moving from opacity to clarity: informing users what data is collected, why, for how long, and with whom it is shared — in language they can actually understand. Consumer behaviour reflects growing scrutiny: 42% now read cookie banners always or often, and 46% accept cookies less often than they did three years ago. This signals that the cookie interaction has become a brand touchpoint, not a formality. Businesses that use Consent Management Platforms (CMPs) to provide accessible dashboards, granular opt-ins, and simple deletion tools build measurable trust advantages. Organisations that hide behind vague legalese do not merely risk regulatory action; they risk abandonment, with 48% of consumers having stopped shopping with a company due to privacy concerns.

2.3 Trade

Modern data protection regimes are not trade barriers — they are trade enablers. By providing a legally predictable and trustworthy framework, regulations such as GDPR facilitate cross-border digital commerce by standardising the conditions under which personal data can flow between jurisdictions. As of 2025, 172 countries — representing 79% of all nations — have enacted data protection laws, a near-universal adoption that reflects the recognition of privacy as a prerequisite for global digital trade.

For businesses, the challenge lies in managing regulatory fragmentation: 76% of Chief Information Security Officers (CISOs) identify multi-jurisdictional compliance as their top challenge. Companies frequently default to GDPR's high standards across all markets for operational consistency, even where lower local standards might technically apply. The cost of non-compliance is steep. IBM's research shows that compliance failures add an average of $1.22 million to breach costs. Yet the returns are clear: 95% of organisations report that the benefits of investing in data privacy exceed costs, with a median return on investment of 1.6x.

3. The Global Regulatory Landscape

The international e-commerce environment is governed by a web of evolving legal frameworks. Understanding their scope, penalties, and strategic implications is essential for any organisation operating across borders.

3.1 GDPR (European Union)

The General Data Protection Regulation remains the global benchmark. Through the so-called "Brussels Effect," it applies extraterritorially to any organisation processing the data of EU residents, regardless of where that organisation is headquartered. It mandates explicit opt-in consent, the right to erasure, data minimisation principles, and breach notification within 72 hours. Penalties reach up to €20 million or 4% of global annual turnover, whichever is greater.

Enforcement has intensified dramatically. From inception in May 2018 through 2025, regulators issued over 2,800 fines totalling more than €6.2 billion — with over 60% of that sum levied since January 2023 alone. In 2025, the pace accelerated further: over 330 fines were issued, generating nearly €1.15 billion in penalties. Ireland, as the lead regulator for many major technology firms, has issued the most impactful fines individually, including a €1.2 billion penalty against Meta in 2023 for unlawful transatlantic data transfers, and a €530 million fine against TikTok in 2025 for transfers to China. The most common violations triggering fines include lack of valid consent, insufficient transparency, inadequate security measures, and improper international data transfers.

3.2 CCPA / CPRA (United States)

The United States lacks a unified federal privacy law, but momentum at the state level is accelerating. As of early 2026, more than 20 states have enacted comprehensive privacy legislation, with Indiana, Kentucky, and Rhode Island's laws taking effect in January 2026. California's Consumer Privacy Act (CCPA), as expanded by the CPRA, remains the most influential U.S. framework, emphasising consumer rights including the ability to opt out of the sale of personal data, the right to correct inaccurate data, and enhanced protections for sensitive categories. Enforcement has been increasing: the U.S. is now the most expensive country in which to suffer a data breach, with an average cost of $10.22 million in 2025 — more than twice the global average.

3.3 India's DPDP Act

India's Digital Personal Data Protection Act represents one of the most significant new privacy frameworks globally, covering a population of over 1.4 billion people. The Act emphasises consent for digital personal data processing and mandates fiduciary accountability for data controllers, with penalties reaching up to ₹250 crore (approximately $30 million). Its enactment signals India's intent to align with global data governance norms while asserting control over cross-border data flows involving its residents.

3.4 Emerging Global Frameworks

Beyond these three anchors, a proliferating set of regimes is reshaping global commerce. Brazil's LGPD (2020), China's PIPL (2021), South Africa's POPIA (2021), and Saudi Arabia's PDPL (2023) each adapt core GDPR principles — consent, purpose limitation, data minimisation — to their own legal and cultural contexts. Together with the forthcoming full application of the EU AI Act in August 2026 — which

introduces fines of up to 7% of global turnover for prohibited AI practices — the regulatory environment is becoming both more comprehensive and more complex to navigate.

4. Real-World Consequences of Data Breaches

Recent high-profile incidents illustrate the full spectrum of financial, operational, and reputational damage that breaches inflict, and validate the systemic importance of supply-chain security.

4.1 Landmark 2025 Incidents in Commerce

- **Marks & Spencer:** Marks & Spencer: A ransomware attack targeting a third-party delivery partner compromised millions of customer records, forced online operations offline for over 72 hours, and triggered regulatory investigations and legal proceedings. The incident exemplified the cascading risk of third-party vendor relationships.
- **Harrods:** Harrods: Approximately 430,000 records were accessed via a third-party provider vulnerability. The breach prompted intensive supply-chain audits and heightened regulatory scrutiny across the luxury retail sector.
- **Louis Vuitton & Adidas:** Louis Vuitton & Adidas: Both brands experienced breaches exposing hundreds of thousands of customer records through weaknesses in vendor and customer support systems, reinforcing the theme that the attack surface extends well beyond an organisation's own infrastructure.

4.2 The Evolving Breach Landscape

IBM's 2025 report reveals that ransomware was present in 44% of all breaches, up from 32% the prior year. When attackers exfiltrated data, the average extortion cost reached $5.08 million. In 1 in 6 breaches, attackers used artificial intelligence, most commonly for phishing (37% of AI-assisted attacks) and deepfake impersonation (35%). Generative AI has dramatically reduced the time and skill required to mount convincing social engineering campaigns.

Despite growing investment in detection capabilities — AI and automation tools cut the breach lifecycle by 80 days and saved nearly $1.9 million on average for organisations using them extensively — recovery remains a protracted process. Most organisations required more than 100 days to achieve full recovery, with a quarter needing over 150 days. Operationally, 86% of breached organisations reported disruptions including delayed sales, interrupted services, or halted production.

The human cost is equally consequential. A 2025 consumer research study found that 52% of consumers view security as crucial when deciding whether to make a purchase, confirming that the commercial impact of breaches extends far beyond the incident itself. Trust, once eroded, is slow to rebuild: research indicates that lost trust following a breach can alter consumer behaviour for years.

5. The AI Dimension: New Risks, New Obligations

The rapid integration of artificial intelligence into commercial operations has introduced a new and underappreciated dimension of data protection risk. IBM's 2025 findings show that breaches involving "shadow AI" — AI tools used without organisational oversight or governance — cost an average of $4.63 million, approximately $670,000 above the standard incident cost.

The governance gap is profound. 63% of organisations have no formal AI governance policies, and 83% lack technical controls to prevent employees from uploading confidential data — including customer PII and proprietary information — into third-party AI tools, with no audit trail and no ability to delete it once shared. 97% of AI-related breaches occurred in companies lacking proper access controls.

Consumer anxiety reflects these structural vulnerabilities. 70% of consumers report little to no trust in companies to make responsible decisions about AI use in their products, and 92% view generative AI as a fundamentally different business process requiring new risk management approaches. In response, 90% of organisations have expanded their privacy programmes specifically because of AI. Regulators are accelerating their response: the EU AI Act, fully applicable from August 2026, introduces fines of up to 7% of global turnover for prohibited AI practices, creating the theoretical possibility of combined GDPR and AI Act penalties approaching 11% of turnover for organisations that violate both simultaneously.

6. Strategic Mitigation and Best Practices

Effective data protection requires a coordinated approach spanning governance, technology, vendor management, and consumer communication. The following best practices reflect current regulatory expectations and empirical evidence on what reduces breach cost and frequency.

6.1 For Organisations

Governance and Accountability

- **DPO Appointment:** Appoint a Data Protection Officer (DPO) with board-level access and clear authority to drive compliance across business units.
- **AI Governance:** Establish formal AI governance policies covering approved tools, data classification requirements, and prohibited uses. Currently 63% of organisations lack such policies, creating significant legal and financial exposure.
- **DPIAs:** Conduct Data Protection Impact Assessments (DPIAs) before launching new data processing activities, particularly those involving AI, behavioural profiling, or sensitive data categories.

Technical Safeguards

- **Encryption & MFA:** Deploy AES-256 encryption for data at rest and in transit, combined with phishing-resistant multi-factor authentication (MFA) across all systems. IBM's data confirms that organisations without MFA face significantly higher breach costs.
- **AI-Assisted Detection:** Invest in AI-powered detection and response capabilities. Organisations using these tools extensively reduced their breach lifecycle by 80 days and saved $1.9 million on average per incident.
- **Data Minimisation:** Implement data minimisation principles: only collect and retain data that is strictly necessary for stated purposes. Regulators increasingly cite excessive data collection as a standalone violation.

Third-Party Risk Management

- **Vendor Audits:** Conduct rigorous vendor security audits before onboarding and require contractual compliance with the same security standards applied internally. The M&S, Harrods, and Louis Vuitton incidents all originated with third-party weaknesses.
- **Consent Management:** Utilise Consent Management Platforms (CMPs) to provide granular, revocable opt-ins and maintain auditable records of user consent. With 42% of consumers now actively reading consent banners, this is a brand interaction, not a formality.
- **Clear Privacy Policies:** Avoid vague or template-generated privacy policies. Regulators have fined organisations specifically for opaque privacy notices, and 63% of consumers already believe most companies are not transparent about data use.

6.2 For Individual Users

- **Strong Credentials:** Use unique, strong passwords (minimum 15 characters) and enable two-factor authentication (2FA) on all commercial accounts. Password reuse remains a leading vector for credential-stuffing attacks.
- **Breach Response:** Act promptly if a breach is suspected: change credentials and monitor financial accounts within a 72-hour window, mirroring the regulatory notification standard for a reason — swift action contains damage.
- **Early Warning Signs:** Recognise warning signs of account compromise: unexpected logins, locked accounts, unfamiliar transactions, or unexplained file changes. Early detection dramatically reduces recovery time and financial impact.
- **Selective Consent:** Exercise consent mindfully. With 46% of consumers accepting cookies less frequently than three years ago, selective consent is now a mainstream privacy hygiene behaviour.

7. Conclusion

Data protection has completed its transformation from a legal compliance obligation into a core commercial competency and genuine competitive advantage. The empirical evidence is unambiguous: organisations that invest in privacy outperform those that do not, both in breach cost containment and in consumer loyalty. With a median 1.6x return on privacy investment, the business case is no longer debatable.

The regulatory environment continues to intensify in every dimension. GDPR enforcement exceeded €1.15 billion in 2025 alone. The EU AI Act will, from August 2026, add a further layer of obligation and financial exposure. Twenty U.S. states now have comprehensive privacy laws, with more expected. 172 countries worldwide have enacted data protection frameworks. Non-compliance is becoming not merely costly but operationally untenable for businesses with global ambitions.

Three structural shifts will define the next phase of data protection in commerce. First, AI governance — currently absent from 63% of organisations — will become a mandatory foundation, not an optional enhancement. Second, supply-chain data security will move from a peripheral concern to a board-level priority, given that recent high-profile breaches originated almost uniformly at third-party vendors. Third, consumer sophistication will continue to rise: with 53% of global consumers now aware of their country's privacy laws and 42% actively reading consent interactions, privacy literacy is becoming mainstream.

Organisations that treat privacy as a strategic differentiator — not a legal burden — will be best positioned to earn and sustain the consumer trust that underpins long-term commercial success in an increasingly data-conscious global marketplace.

REFERENCES

1. **IBM Security.** *Cost of a Data Breach Report 2025.* IBM Corporation, 2025. https://www.ibm.com/reports/data-breach
2. **All Covered.** *"Key Insights from IBM's 2025 Cost of a Data Breach Report."* All Covered Blog, September 8, 2025. https://www.allcovered.com/blog/key-insights-from-ibms-2025-cost-of-a-data-breach-report
3. **Usercentrics.** *The State of Digital Trust in 2025.* Sapio Research / Usercentrics, November 2025. https://usercentrics.com/knowledge-hub/state-of-consumer-trust-in-2025-report/
4. **Usercentrics.** *150 Data Privacy Statistics for 2025 You Need to Know About.* Usercentrics, March 25, 2025. https://usercentrics.com/guides/data-privacy/data-privacy-statistics/
5. **Cisco.** *2025 Data Privacy Benchmark Study.* Cisco Systems, Inc., 2025. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2025.pdf
6. **Termly / Piirainen, N.** *"64 Alarming Data Privacy Statistics Businesses Must See in 2025."* Termly, March 2, 2026. https://termly.io/resources/articles/data-privacy-statistics/
7. **CDP.com.** *Data Privacy & Brand Trust Statistics (2026).* CDP.com, 2026. https://cdp.com/basics/data-privacy-statistics-brand-trust/
8. **Liquid Web.** *Who Do Americans Trust With Their Data in 2025? The Digital Trust Report.* Liquid Web, September 11, 2025. https://www.liquidweb.com/white-papers/digital-trust-report/
9. **Singh, H., Anand, N., Singh, S., Angirish, N., Sengupta, P. D., & Amin, S.** *"Examining the Impact of Personal Data Breaches on Consumer Trust and Privacy Protection Behavior in E-Commerce."* Advances in Consumer Research, 2(5), 2101–2111, November 25, 2025. https://acr-journal.com/article/examining-the-impact-of-personal-data-breaches-on-consumer-trust-and-privacy-protection-behavior-in-e-commerce-1917/
10. **The Academic.** *"Impact of Digital Privacy Concerns on Consumer Trust and Purchase Intentions in E-Commerce."* Research on Management and Business Economics, 22(2), 2025. https://theacademic.in/wp-content/uploads/2025/10/17-1.pdf
11. **Metastat Insights.** *Data Privacy Market Size, Growth & Share Analysis by 2033.* Metastat Insights, April 2, 2025. https://metastatinsight.com/report/data-privacy-market
12. **Aspen Digital, Consumer Reports & Global Cyber Alliance.** *2025 Consumer Cyber Readiness Report.* Aspen Digital, October 1, 2025. https://www.aspendigital.org/report/2025-consumer-cyber-readiness-report/
13. **Surfshark.** *GDPR Breaches Led to Over €1B in Fines in 2025.* Surfshark Research, January 20, 2026. https://surfshark.com/research/study/gdpr-fines-2025
14. **Data Privacy Manager.** *20 Biggest GDPR Fines So Far [2025].* Data Privacy Manager, March 4, 2025. https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
15. **Infosecurity Magazine.** *"The 10 Biggest Data Breach Fines and Settlements of 2025."* Infosecurity Magazine, December 26, 2025. https://www.infosecurity-magazine.com/news-features/top-10-data-breach-fines-2025/
16. **Scrut.io.** *Avoiding GDPR Fines in 2025: Enforcement Trends and Tips.* Scrut.io, November 5, 2025. https://www.scrut.io/hub/gdpr/gdpr-fines-penalties-us-eu-guide
17. **ComplyDog.** *Biggest GDPR Fines of 2025.* ComplyDog Blog, 2025. https://complydog.com/blog/biggest-gdpr-fines-of-2025
18. **CookieScript.** *GDPR Enforcement: Complete Guide for 2025.* CookieScript, September 23, 2025. https://cookie-script.com/guides/gdpr-enforcement
19. **DeepStrike.** *Data Breach Statistics 2025–2026: Global Trends & Costs.* DeepStrike Blog, 2025. https://deepstrike.io/blog/data-breach-statistics-2025
20. **StationX / House, N.** *Data Privacy Statistics [2026]: 51+ Laws, Fines & Trends.* StationX, 2026. https://app.stationx.net/articles/data-privacy-statistics
21. **European Parliament and Council of the European Union.** *Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR).* Official Journal of the European Union, May 4, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
22. **State of California.** *California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA).* California Civil Code §1798.100 et seq., 2018 (amended 2020). https://oag.ca.gov/privacy/ccpa

23. **Ministry of Electronics and Information Technology, Government of India.** *The Digital Personal Data Protection Act, 2023.* Gazette of India, August 11, 2023. https://www.meity.gov.in/content/digital-personal-data-protection-act-2023
24. **CMS.Law.** *GDPR Enforcement Tracker.* CMS Law Tax and Advisory, updated continuously. https://www.enforcementtracker.com/
25. **DLA Piper.** *GDPR Data Breach Survey 2026.* DLA Piper International LLP, 2026. https://www.dlapiper.com/en/insights/publications/2026/01/gdpr-data-breach-survey-2026
26. **World Economic Forum.** *Global Cybersecurity Outlook 2025.* WEF, January 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/
27. **Pew Research Center.** *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information.* Pew Research Center, November 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
28. **Greenleaf, G.** *"172 Countries Now Have Data Privacy Laws — 79% of the World's Nations."* Privacy Laws & Business International Report, 2025. https://www.privacylaws.com