The Indian Journal for Research in Law and Management


Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896



# DATA PROTECTION LAWS AND THE DIGITAL ECONOMY: BALANCING PRIVACY

***Gunja Nehra***

Every time we search for something online, buy a product, or scroll through an app, we leave behind a trail of personal information. Countries now pass laws to secure information that people provide. That information is used by corporations to show ads to customers, and also by banks to decide who is worthy of receiving loans. In fact, data today is something like raw material for oil and steel. People give away their personal data although it is precious, and therefore, the European, American, and Indian governments have introduced legislation that safeguards users' data. The legislation includes the introduction of the European Union's General Data Protection Regulation, the California Consumer Privacy Act, and the Digital Personal Data Protection Act of 2023 in India. That's the balance this paper is really about. And honestly, the more I read into this, the more I think it's not as simple as "privacy laws cost money and hurt the economy." It's more that these laws move money around; some businesses lose, some win, and overall, trust between companies and their customers can actually go up.

## HOW THESE LAWS ACTUALLY WORK

The basic philosophy behind these laws is that privacy shouldn't just be something you sue over after your data gets misused; it should be protected before anything goes wrong. GDPR, which kicked in back in 2018, says companies can only collect data for specific reasons, shouldn't collect more than they need, and have to be able to show they're being responsible with it. If a

company messes this up, the fine can go up to €20 million or 4% of their entire global revenue, whichever is bigger[1]. And it doesn't matter where the company is based; if it deals with people in the EU, GDPR applies to it[2]. That's a huge deal, and it's basically why so many other countries copied this model when writing their own laws.

India's DPDP Act is built on a similar idea but adjusted for India's own situation. It sets up a Data Protection Board to handle complaints, has extra rules for really big companies that process huge amounts of data (the law calls them "Significant Data Fiduciaries"), and only allows sending data abroad if the government hasn't specifically restricted that country.[3] What's interesting is that India isn't switching all this on at once; it's being rolled out in stages. The Data Protection Board actually started functioning in November 2025, a system for approving "Consent Managers" (basically companies that help you manage your data permissions) kicks in around November 2026, and the real teeth of the law, breach reporting, data rights, all of it only becomes enforceable in May 2027[4]. I think this staggered approach makes sense; it gives smaller businesses breathing room instead of hitting them with everything overnight. And the legal groundwork for all of this goes back to a 2017 Supreme Court of India ruling, which said privacy is a fundamental right under the Constitution, a pretty landmark decision[5].

The U.S. is a weird case in comparison, because there's no single national privacy law at all. Instead, there's a mess of different state laws, with California's CCPA leading the pack[6]. In practice, this means companies just end up following whichever state's rules are strictest, everywhere, because that's easier than tracking fifty different standards. So in a roundabout way, even states with no privacy law of their own still end up protected by something that looks a lot like GDPR just imported through the back door.

## THE COST SIDE - BECAUSE YES, THIS STUFF IS EXPENSIVE

It would be dishonest to pretend these laws don't cost real money, because they do. Right after GDPR passed, early estimates suggested a small European company might have to spend several hundred thousand dollars just to hit the minimum requirements. More recent numbers

[1] Regulation 2016/679, art. 83, 2016 O.J. (L 119).
[2] Regulation 2016/679, art. 3, 2016 O.J. (L 119) (establishing extraterritorial scope).
[3] Digital Personal Data Protection Act, No. 22 of 2023, 8, 16, 18, India Code (2023).
[4] India's Digital Personal Data Protection Regime Takes Effect, Lexology (Nov. 24, 2025); India Passes the Digital Personal Data Protection Rules, Privacy World (Nov. 26, 2025).
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1; W.P. (C) No. 494 of 2012; AIR 2017 SC 4161 (India).
[6] California Consumer Privacy Act of 2018, Cal. Civ. Code 1798.100 - 1798.199 (West 2018).

are even bigger. Some large companies reportedly spend up to $70 million a year just keeping up with GDPR compliance[7].A 2024 study by Chen, Frey, and Presidente[8] found that on top of the direct costs, GDPR also made it harder for companies to get new data, cut down cross-border data flow, and slowed investment in industries that depend heavily on data. There's also research showing that weekly venture capital funding into European tech startups actually dropped after GDPR came in, because investors started pricing in compliance risk when deciding what a company was worth[9].

And this cost isn't spread evenly at all. Smaller businesses get hit way harder relative to their size than big companies do. One study found that small IT firms lost a much bigger chunk of their profits post-GDPR compared to larger IT firms[10]. Which, if you think about it, is kind of ironic, these laws were partly meant to rein in giant tech companies, but if only the giants can afford the compliance overhead, it might end up protecting their market position instead of challenging it.

Enforcement has ramped up a lot, too. GDPR fines have added up to more than €6 billion since the regulation took effect in 2018[11]. Some critics have half-jokingly called it a "digital tax" on doing business across borders. Fair or not, that number tells you regulators aren't treating this as some minor paperwork issue anymore. It's a serious cost of doing business now.

**BUT THERE'S A REAL UPSIDE TOO**

Here's the thing, though - there's solid evidence that these laws also create real economic value. It's just harder to see because it doesn't show up as neatly as a compliance bill does. Personal data is a strange kind of economic good: it costs something to create in the first place, it's not really bought and sold like a normal product, but once it exists, copying it costs almost nothing. That's exactly the kind of situation where things go wrong without rules in place - companies have little reason to be careful with data if there's no cost to misusing it, kind of like how

[7] Jimenez-Hernandez, Demirer & Peng, Data, Privacy Laws and Firm Production: Evidence from the GDPR (Fed. Trade Comm'n, cited 2018) (finding compliance costs ranging from $1.7 million for small/medium firms to $70 million for large enterprises).
[8] Chinchih Chen, Carl Benedikt Frey & Giorgio Presidente, Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally, Econ. Inquiry (2024).
[9] Jian Jia, Ginger Zhe Jin & Liad Wagman, The Short-Run Effects of GDPR on Technology Venture Investment, 40 Marketing Sci. 661 (2021) (NBER Working Paper No. 25248, 2018).
[10] Chen, Frey & Presidente, supra note (finding a 12.5% profit decline for small IT firms compared to 4.6% for large IT firms).
[11] CMS, GDPR Enforcement Tracker Report 2025/2026 - Numbers and Figures (Mar. 2026) (recording approximately €6.11 billion in cumulative GDPR fines since 2018).

factories won't bother controlling pollution unless a law forces them to. Data protection law is basically a fix for that problem.

It's also created entirely new industries. According to projections, the worldwide market for privacy technology and compliance tools is expected to reach around $50.8 billion by the year 2034, with approximately 60% of companies now defining privacy-by-design as a source of competitive advantage rather than an obligation under the law. Global expenditure on cybersecurity and risk management reached 212 billion USD in 2025[12], with a considerable rise in stock prices among companies specializing in compliance and security tools as well. The point here is that although regulations cost businesses money today, they have created a whole industry of organizations that operate in the compliance-focused market. It should be noted that there is also a phenomenon that can be called a trust bonus; surveys show that the companies that take data protection seriously generally retain customers for a longer period. France's data protection authority reviewed five years of GDPR and concluded that, despite the real costs, it helped build a foundation of trust that benefits everyone in the market by cutting down the uncertainty users feel about what happens to their data[13].

## A REAL CASE: META'S €1.2 BILLION FINE

To make this less abstract, it's worth looking at one actual case - probably the most famous GDPR enforcement action so far. In May 2023, the Data Protection Commission of Ireland imposed a fine of €1.2 billion, approximately $1.3 billion, on Meta (the parent company of Facebook and Instagram) for sending the private data of users in Europe to the USA in an irresponsible manner[14]. This is, to date, the highest penalty under the GDPR, beating the previous record of €746 million, which was charged to Amazon[15]. The roots of this story date back almost ten years, when in 2013 Austrian privacy advocate Max Schrems claimed that European data transmitted to US servers was subject to access by American intelligence agencies without the layers of legal protection guaranteed to individuals by EU legislation. As a result, the European Union Court issued two important decisions, which are known as Schrems I and Schrems II, and ruled that previous regulations allowing the transfer of data between the EU and the USA were no longer valid because the US regulations do not provide "essentially

[12] Gartner, Inc., Gartner Forecasts Global Information Security Spending to Grow 15% in 2025 (Aug. 28, 2024).
[13] Commission nationale de l'Informatique et des Libertés (CNIL), The Economic Impact of GDPR, 5 Years On (2023).
[14] Data Protection Commission, Data Protection Commission Announces Conclusion of Inquiry into Meta Ireland (May 22, 2023); Irish Regulator Fines Meta 1.2 Billion Euros and Orders It to Cease Data Transfers to the U.S., Hunton Privacy & Info. Sec. L. Blog (May 22, 2023).
[15] Irish Data Protection Commissioner Imposes a €1.2 Billion Fine on Meta Ireland, BDO (2023).

equivalent" protection[16]. Trying to solve this problem, Meta employed standard clauses for contracts and added other protective measures, but the regulators did not agree that this solution was adequate. Along with the fine, Meta was ordered to stop sending EU data to the U.S. within five months and clean up or delete data that had already been transferred unlawfully since mid-2020 - which, given how tangled Meta's global infrastructure is, was genuinely a massive operational headache, not just a fine to write a check for[17].

What I find interesting about this case is that it kind of proves both sides of the argument at once. On one hand, it shows how brutal GDPR penalties can get and how disruptive enforcement can be to actual business operations, not just the bottom line. On the other hand, it's also proof that the law works the way it's supposed to - one activist and a decade of legal fights managed to hold a trillion-dollar company accountable in a way that would've been nearly impossible without a strong legal framework backing it up. It even pushed the EU and U.S. governments to negotiate a fresh data-transfer agreement, which shows privacy enforcement doesn't just affect one company - it can reshape entire international policies.

**SO IS IT A TRADE-OFF OR NOT?**

Putting all this together, I don't think privacy laws just shrink the digital economy - they redirect where the money flows. Companies that made money by using people's data however they wanted, like data brokers and ad-tracking networks, tend to lose out. Meanwhile, companies that can build actual trust - privacy-focused tech firms, compliance consultants, platforms that are upfront about their data practices - tend to gain. There are real winners and losers here, and without careful design, the gap between big, well-funded companies and small, cash-strapped startups is probably going to widen. That's part of why staggered approaches, like India's rollout timeline or lighter rules for smaller companies in the EU, actually matter - they're trying to stop smaller players from getting crushed in the process.

Then there's AI, which complicates everything even further. AI models need enormous amounts of data to train on, and a lot of that data was originally collected for one purpose and then reused for training - which directly clashes with the basic privacy principle that data should only be used for what it was collected for. Regulators in both the EU and India are still figuring out how consent-based rules, built for simple one-time data exchanges, are supposed to apply to systems that are constantly learning from massive data pools. Honestly, this feels like the biggest

[16] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559 (July 16, 2020).
[17] Irish Regulator Fines Meta 1.2 Billion Euros and Orders It to Cease Data Transfers to the U.S.

unresolved question in privacy law right now and has huge consequences for the AI industry, which increasingly sits inside a digital economy that already makes up around 10% of the entire U.S. economy[18].

## WHAT MIGHT ACTUALLY WORK BETTER

Based on everything above, a few ideas seem worth pushing for. Rolling out rules slowly, as India did, gives the market time to adjust instead of causing a sudden shock to startup funding. Scaling requirements to risk - so companies handling more sensitive or larger amounts of data face tougher rules than small businesses barely touching any - would help fix the unfair burden that flat compliance costs currently put on smaller firms. And governments could actually treat the privacy-tech industry as a policy tool instead of an accidental side effect, maybe by subsidizing compliance software for small businesses instead of just leaving them to figure it out on their own.

## CONCLUSION

At the end of the day, privacy law and the digital economy aren't really enemies fighting a zero-sum battle, even though it's often framed that way. Looking at nearly a decade of GDPR and India's newly active DPDP framework, the actual picture is messier than a simple trade-off: yes, there are real costs, and yes, they land harder on smaller businesses. But there are also new markets being created, a genuine boost in trust for companies that get compliance right, and a long-term fix for the fact that personal data is valuable but was, for a long time, barely protected at all. The real challenge going forward isn't picking privacy over growth or the other way around - it's designing these laws carefully enough so that the costs don't fall unfairly on the people least able to afford them, while the benefits of a more trustworthy digital economy are shared more broadly.

[18] U.S. Bureau of Econ. Analysis, New and Revised Statistics of the U.S. Digital Economy, 2005–2021 (2022) (reporting the digital economy at 10.3% of nominal GDP in 2021).