TEFMJ TRENDS IN ECONOMICS, FINANCE AND MANAGEMENT JOURNAL

Data Breaches in the Telecom Sector: A Comparative Analysis of Regulatory Fines Across Continents

Anjali Gupta, N.P Singh

DOI: https://doi.org//10.69648/WWJV4418

Trends in Economics, Finance and Management (TEFMJ), 2026; 8(1): 47-72

ijtns.ibupress.com

Online ISSN: 2671-3365

Application : 18.04.2026

Revision : 19.05.2026

Acceptance : 23.06.2026

Publication : 26.06.2026

Gupta, A., & Singh, N. P. (2026). Data breaches in the telecom sector: A comparative analysis of regulatory fines across continents. Trends in Economics, Finance and Management Journal, 8(1), 47-72. https://doi.org//10.69648/WWJV4418

Anjali Gupta[1], N.P Singh[2]

[1] School of Business Management & Commerce, MVN University, Palwal-121105, Haryana, India, https://orcid.org/0009-0002-8027-8362

[2] School of Business Management & Commerce, MVN University, Palwal-121105, Haryana, India, https://orcid.org/0000-0002-3006-9522

Correspondence concerning this article should be addressed to Anjali Gupta

Email: 22ms9002w@mvn.edu.in & anjalgupta14august@gmail.com

BALKAN JOURNALS

Abstract

The research paper examines the incidences of telecom data breaches, and regulatory measures that have been taken in the chosen countries of Asia, Europe, North America, Africa, and especially in Indian telecom sector. As the world moves at a fast pace towards digitalization, higher mobile penetration and high use of online services, telecom operators deal with huge amounts of personal data, and data breaches are becoming a major challenge to regulators across the globe.

The study applies a comparative qualitative approach to the investigation of the response to cybersecurity incidents by different jurisdictions using documented breach incidents and publicly reported regulatory actions. The results indicate a significant difference between regulators in Europe and North America, who tend to impose huge financial fines after big data breaches and those in India who have been mostly using advisories, notices and compliance audits with small financial fines.

The paper presents a point where variations in legislations, regulatory ability, and level of data protection systems affect enforcement strategies. The Digital Personal Data Protection Act, 2023, introduced in India, provides an opportunity to strengthen the country's telecom data protection framework and align it with international standards.

Keywords: Telecom Data Breaches, Data Protection Regulation, Cybersecurity Governance, Telecom Sector Regulation, Digital Personal Data Protection Act.

Introduction

In the digital age, telecommunications networks are part of the critical infrastructure, processing huge volumes of sensitive and personal data, as well as operational data. The growing dependence on the mobile and broadband services has rendered telecom operators one of the prime targets of cyberattacks, which puts the personal data of millions of users in danger of being misused. Such high-profile cases as the SK Telecom attack in 2025, which leaked the information of close to 27 million subscribers, demonstrate that telecom systems are susceptible and need strict regulation (Reuters, 2025a; ETTelecom, 2025). These violations do not only affect the privacy of individuals but also undermine the confidentiality and reliability of national communication systems.

The reaction of the regulatory authorities to data breaches, though, greatly differs in different regions. The Personal Information Protection Commission (PIPC) in South Korea fined SK Telecom USD approximate of 96.5 million, a record fine, proving that the strict enforcement method put in place to curb corporate laxity is effective (Reuters, 2025b). Conversely, in India, violations at state-owned telecommunication companies like BSNL have been met with minimal or no punishment in most cases indicating the weaknesses in enforcement abilities and the maturity of information protection systems (ETTelecom, 2024). These differences shed light on the essential research gap: the risk of data breaches is a universal concern not only internationally but also the regulation intervention with its effectiveness and rigor varies significantly, which has a certain impact on corporate compliance.

The situation is quite different in Europe, as a new set of laws known as the General Data Protection Regulation (GDPR) has created one of the most detailed legal frameworks on data protection in the world. Telecom operators are also liable to heavy fines and remedies under GDPR in case of data breach as seen in fines given to operators like BT Group and Vodafone Spain (Termly, 2026). On the same note, regulatory bodies in North America such as the Federal Trade Commission (FTC) and Federal Communications Commission (FCC) are also active in the application of data privacy-based regulations, the most prominent examples being the USD177 million settlement of AT&T after a massive data breach (Reuters, 2025b). These powerful enforcement mechanisms can create a distinct preventive impact, motivating telecom operators to implement more effective cybersecurity policies and proactive data protection practices.

The academic literature also highlights the importance of regulatory oversight to reduce the risk of corporate data breach. Research shows that strict regulations do not only decrease the rate of breaches but also increase the preparedness of the organization by facilitating the culture of governance and compliance (Gao et al., 2025). Regardless of these observations, there is little research that has comparatively examined regulatory reactions in Asia, Europe, North America and Africa in the telecom sector. To address this gap, this research paper will provide a cross-continent comparative analysis of the data breaches, regulatory measures, and fines imposed on the telecom operators. Through the study of disparities in enforcement, legal frameworks, and regulatory effectiveness, this study aims to offer practical information on policymakers, telecom regulators and industry participants.

Literature Review

According to the literature, telecommunications companies are at an increased risk of data breaches since they collect and process significant amounts of personal and metadata information, which is vulnerable to breaches. Previous studies single out regulatory enforcement and the severity of penalty as the major factors of corporate cybersecurity behaviour, but telecom-specific cross-continental comparison is scarce.

Telecom Data Breach Risks

Telecommunication companies form an essential unit of digital infrastructure and handle high amounts of sensitive data of customers every day, such as personal identification data, call data records, location metadata, and Know Your Customer (KYC) documents. Previous scholarly studies repeatedly attribute the telecommunication industry as one of the riskiest industries when it comes to data breaches because of its centralized data architecture and high levels of third-party integrations (Anderson et al., 2013). This is confirmed empirically by Romanosky (2016), who shows that the breach frequency is disproportionately higher in industries that deal with large amounts of consumer data, and telecom companies are especially vulnerable to the risks of identity theft and surveillance.

However, academic sources also indicate that cases of telecom data breach are mainly due to the poor governance of cybersecurity, outdated IT systems, and lack of vigilance on vendor access (Böhme & Moore, 2012). Research on breach typologies points out that the privacy risk presented by unauthorized access to call logs

and metadata is more serious than the risk posed by financial data breaches since such information can be used to make behavioral predictions and conduct long-term monitoring (Acquisti et al., 2016). These results are consistent with actual telecom breaches in Asia, Europe, and North America where personal and metadata breach is the most common breach event.

Regulatory Frameworks Governing Telecom Data Protection

The regulatory approaches in telecom data protection differ greatly depending on jurisdictions. The General Data Protection Regulation (GDPR) is a complex legal rule in Europe that puts telecom operators under strict responsibility in terms of minimizing data, notifying about breaches, and responsibility. Kuner (2022) states that GDPR has essentially altered the application of data protection by applying administrative fines derived based on international turnover, creating a stricter regulation of data-driven industries like telecommunications. Empirical evidence indicates that GDPR has enhanced organization awareness and compliance investment, particularly in high-risk sectors (Wolters, P. T. J, 2019).

Telecom data protection in the United States is regulated through a fragmented regulatory framework that involves sector-specific regulation by the Federal Communications Commission (FCC) and more general consumer protection regulation by the Federal Trade Commission (FTC). A study by Greenstein, S., & Prince, J. (2015) concludes that the U.S. telecom companies are more responsive to the litigation risk and settlement expenses compared to regulatory penalties, meaning that the market-based compliance system is in place instead of a cohesive statutory regime.

The Asian regulatory systems are incredibly heterogeneous. South Korea has established one of the most restrictive personal data protection systems in Asia, which is backed by operating institutions of enforcement and administrative penalties (Greenleaf, G. (2021). On the other hand, the telecom data protection in India was based on the sectoral guidelines and contractual obligation in the past, and the sanctions were not actively used to prevent data breach until the implementation of the legislation on data protection. Research into the data governance model in China observes that although the laws governing data control are the most comprehensive, there is a lack of transparency in enforcement, especially in telecom companies related to the state (Creemers, R. 2022). These differences provide an unequal incentive to compliance within the Asian telecom markets.

Fines, Enforcement, and Deterrence

Deterrence theory provides a strong explanation of the relationship between regulatory fines and corporate cybersecurity behaviour. According to the economic model of deterrence by (Becker, 1968), as the expected penalties are raised, the compliance will be higher as the cost of violation is also increased. Using this framework, Romanosky et al. (2011) found that the higher the enforcement regime, the more both companies tend to invest in preventive cyberspace controls.

The recent cross-industry research proves that regulatory fines are influential in avoiding the recurrence of breaches, especially when the fines are high and regularly imposed (Kamiya et al., 2021). This deterrence mechanism can be illustrated by the example of GDPR implementation in Europe where telecom operators could pay penalties in the form of millions of euro in case of non-compliance. On the other hand, studies show that symbolic enforcement measures, i.e. warnings or advisories with no financial penalties, do not have much effect in terms of long-term cybersecurity investment (Böhme et al., 2019). This observation is specifically applicable in Asian telecom markets where regulatory actions will tend not to have financial sanctions (Becker, 1968).

Comparative Studies: Asia, Europe, and North America

According to comparative academic studies on data protection enforcement, regions have been contrasted sharply. In European literature, compliance is ensured through rules and is centralized, whereas in North American literature, market discipline, lawsuits, and reputational loss are paramount (Gal-Or et al., 2018). Asian studies, in turn, tend to be more interested in regulatory capacity building instead of the enforcement results (Greenleaf, G. (2021).

In spite of these contributions, there are limited comparative studies on telecom. Majority of the current literature lumps telecom companies under more general information services or technology groups, which ignores the sector specific enforcement dynamics. Consequently, only limited direct comparisons of telecom data breach penalties have been developed in the literature in the Asia, Europe, and North America.

Gaps in the Literature

There are three significant gaps in the review. To begin with, the majority of empirical research studies the incidences of data breach at the macro level of the industry, as opposed to concentrating on the telecom industry. Second, there are limited

cross-continental comparative studies that incorporate the results of enforcement and the severity of punishment. Third, there is lack of concern about the viability of regulatory fines in the latest Asian telecom markets compared to the developed European and North American systems. To fill these gaps, the current paper will make a comparative study of telecom data breaches and policymaking in Asia, Europe, North America, and Africa in order to determine whether tougher punishments result in better compliance.

Research Methodology

Research Design

This study uses a descriptive and comparative research design, to analyse incidences of data breach in the telecommunications industry and the regulatory measures taken in Asia, Europe, North America and Africa. The study is largely qualitative with a background of descriptive quantitative data regarding breach events and enforcement effectiveness. This is a suitable strategy in the examination of the institutional variation in regulatory enforcement and compliance practice across jurisdictions, especially in the emerging and the advanced telecom markets.

Its aim is on the analysis of the reaction in the regulator against the breach of telecom data, instead of quantifying the level of performance in firms or developing predictive models.

Scope of the Study

The current paper analyses major telecom data breach incidents and regulatory responses across selected countries in Asia, Europe, North America and Africa between 2020 and 2025. The European nations used in the analysis include the United Kingdom, Italy, Spain, Germany, Sweden, Norway, Denmark and Finland whereas Asian nations used in the research include South Korea, India, Sri Lanka, China and Nepal. The focus of the research will be limited to publicly announced cases of data breaches related to customer personal information, such as KYC data, call logs and metadata and other sensitive subscriber data. The telecom operators, both states owned and those owned by individuals, are taken into account to capture the potential variation in regulatory responses, enforcement and compliance practices in different institutional and regulatory settings. Selected African countries including South Africa and Kenya were also included to provide a broader cross-continental comparison.

Data Sources

This paper relies entirely on secondary data collected by authoritative sources that are publicly available. Data on the cases of telecom data breaches and the corresponding regulatory actions were gathered by reviewing the official publications of national data protection authorities, telecommunications regulatory agencies, and the enforcement agencies in Asia, Europe, North America, and Africa. Corporate disclosures, annual reports and transparency statements issued by telecom operators were also used to draw additional data. As a supplement to the analytical basis, the published academic work on data breaches, cybersecurity governance, and regulatory enforcement in the telecommunications and information infrastructure fields was also studied. It used only verifiable and credible sources to have uniformity, accuracy, and reliability of data utilized in the study. No primary data collection was done.

Method of Analysis

The analysis adopts a comparative and descriptive approach to examine telecom data breach incidents and regulatory enforcement practices across different regions. Initially, publicly disclosed data breach cases were compiled and categorized based on the nature of the breach and the type of regulatory response. Subsequently, regulatory actions taken in Asia, Europe, North America and Africa were compared to identify differences in enforcement intensity, penalty structures, and institutional approaches. The findings were then interpreted thematically to assess how variations in regulatory frameworks and enforcement capacity influence data protection outcomes in the telecommunications sector. This qualitative comparative method enables a structured evaluation of cross-regional differences without relying on statistical modelling.

Ethical Considerations

The research is conducted using publicly available information only and does not entail human subjects or confidential data. There was no need thus of an ethical approval. Sensitive operational information that is already available in the market was not disclosed.

Limitations of the Study

The research is vulnerable to some limitations. The variation in data breach disclosure standards in various jurisdictions can have an impact on the quality of

information disclosed. Further, other regulatory activities-especially informal or non-public enforcement measures- cannot be reflected in the records.

Analysis of Telecom Data Breaches

In this section, the similarities and differences between telecom data breach events and the regulatory actions across various parts of the world are described. The discussion is on the reaction of telecom regulators to data breaches especially in terms of imposing penalties on telecom operators in terms of fines. The study emphasizes the differences between regulatory practices and institutional approaches to data protection regulations by analysing examples of the Asian, European, North American, and some African markets.

Telecom Data Breaches in Asia

Data breaches in telecom have been on the rise in various Asian nations, and its occurrence is indicative of the emergent cybersecurity threats in fast-growing digital communication channels. The regulatory reactions in the region are highly diverse based on the capacity of a country and the national legal framework.

The table below shows some of the telecom data breach cases and their respective regulatory measures in the Asian countries. The comparison shows differences in the enforcement strategies especially concerning the application of monetary punishments.

Table 1:

Telecom Data Breaches and Regulatory Responses in Selected Asian Countries

Country	Year	Nature of Data Breach	Action of Regulator	Telecom Company	Fine Imposed
South Korea	2025	Personal data leak of ~27 million subscribers	Heavy monetary penalty	SK Telecom	USD 96.53 million
India	2025	Alleged subscriber data exposure	No penal action	BSNL	No monetary fine
India	2024	Customer KYC & mobile data leak allegations	Advisory issued	Bharti Airtel	No monetary fine

Country	Year	Nature of Data Breach	Action of Regulator	Telecom Company	Fine Imposed
India	2023	Unauthorized access via third-party apps	Clarification sought	Reliance Jio	No monetary fine
India	2023–24	SIM & KYC compliance lapses	Notice issued	Vodafone Idea (Vi)	No monetary fine
India	2024	Customer data security concerns	Advisory only	MTNL	No monetary fine
India	2022	Cybersecurity incident	Internal audit	RailTel Corporation	No monetary fine
Sri Lanka	2022	Customer metadata exposure	Warning issued	Dialog Axiata	No monetary fine
China	2022	Internal user data leak	Compliance audits	China Mobile	Not disclosed
Nepal	2021	Subscriber data breach	Regulatory notice	Ncell	No fine

Source: Reuters (2025a); Greenleaf, G. (2021); HT Digital Streams Ltd. (2024); Bharatnet (2024); GSMA Intelligence (2024); TeleGeography (2023); & Times of India. (2023 & 2024).

Note: "Not Disclosed" indicates that regulatory authorities did not publicly disclose the monetary value of the penalty in available official reports.

Table 1 shows the cases of telecom data breach and regulatory actions in the case of the Asian countries of choice. The analysis shows that there is a lot of variation in the practice of enforcement in the region. South Korea shows a rather good enforcement system, in which the authorities have fined SK Telecom with a large amount of money using the breach of a large amount of data of millions of customers (Reuters, 2025a).

Conversely, the regulatory reactions in other countries like India and Sri Lanka have majorly been based on advisory actions and inspections and not on monetary sanctions. A number of telecom providers in India such as BSNL, Bharti Airtel, Reliance Jio, Vodafone Idea, MTNL and RailTel Corporation were subject to regulatory reviews after cybersecurity attacks. Nevertheless, they were overlooked by

regulatory notice, advisory, or internal audit, rather than fined (Business Standard, 2024; PRS Legislative Research, 2023; BharatNet, 2024).

Generally, the results suggest that regulatory implementation in all Asian telecom markets is more of a compliance-based approach as opposed to the deterrence approach. Some nations are slowly enhancing data protection laws, although the lack of uniform monetary fines might weaken the motivation of telecom operators to engage in more intense cybersecurity activities (Greenleaf, G. 2021; Gao et al., 2025).

Some cases, such as Bharti Airtel and Reliance Jio, involved alleged or disputed data breaches. These cases are included to examine regulatory responses rather than confirmed regulatory violations.

Telecom Data Breaches in Europe

In European telecom markets, there is a more restrictive regulatory environment as far as the enforcement of data protection is concerned. With the implementation of the General Data Protection Regulation (GDPR), regulatory powers have become much stronger and corporations have become more responsible in terms of personal data protection.

The table below highlights the key cases of data breaches by major telecoms in Europe and regulatory measures implemented in the chosen countries. These instances exemplify the robust deterrence-based enforcement model that defines European data protection governance.

Table 2.

Telecom Data Breaches and Regulatory Responses in Selected European Countries

Country	Year	Nature of Data Breach	Telecom Company	Regulatory Action	Fine Imposed
UK	2023	Personal data leak (~2 million users)	BT Group	GDPR enforcement	£1.1 million
Italy	2020	Subscriber KYC data exposure	TIM	GDPR penalty	€27.8 million
Spain	2021	Unauthorized access to customer accounts	Vodafone Spain	GDPR enforcement	€8.15 million

Country	Year	Nature of Data Breach	Telecom Company	Regulatory Action	Fine Imposed
Germany	2022	Data leak through mobile application	Deutsche Telekom	GDPR fine	€17 million
Sweden	2021	Customer data protection violation	Tele2	Regulatory action	€1 million
Norway	2022	Telecom security breach	Telenor	Enforcement action	NOK 4 million
Denmark	2020	Personal data breach via telecom platform	TDC Group	Compliance order	DKK 1.2 million
Finland	2021	Subscriber data protection violation	Elisa Oyj	Data protection ruling	€ 9,00,000

Source: Reuters (2022, 2023, 2024); European Data Protection Board (2024); ICO Annual Report (2023); GSMA Intelligence (2024).

Table 2 highlights the cases of telecom data breaches and enforcement in some of the European countries selected. Table 2 shows that the European regulators' policy is more stringent and regulatory in the implementation of the General Data Protection Regulation (GDPR). The European GDPR policy allows the regulators to have the legal power to issue a large fine to companies that do not make sufficient efforts to comply with data protection (Kuner, 2022).

There are a number of telecom companies which have been charged with a high penalty for the violation of customers' data. For example, Telecom Italia (TIM) had been fined by the European data protection regulators up to 27.8 million for violating the data protection, while Vodafone Spain and Deutsche Telekom had also been fined for the breach of consumer data security. This enforcement was based on the high deterrence mechanism of GDPR (European Data Protection Board, 2024).

Unlike many Asian countries, European regulators have always been levying fines in case of a violation of data protection despite the size or ownership of telecom entities. Such a consistent set-up of enforcement will encourage many telecom companies to adopt cyber security and data protection measures (Wolters, P. T. J, 2019).

The Nordic countries also demonstrate a strong commitment to GDPR-based enforcement. Sweden's Tele2, Norway's Telenor, Denmark's TDC Group, and Fin-

land's Elisa Oyj were subject to regulatory actions relating to customer data protection and telecom security. Although the monetary penalties imposed in these countries were generally lower than those observed in larger European economies such as Italy, Germany, and Spain, the enforcement approach remained consistent with GDPR principles. These cases indicate that even smaller digital economies prioritize accountability, transparency, and proactive compliance in telecom data governance.

Telecom Data Breaches in North America

Telecom data protection enforcement in North America is frequently a mixture of regulatory control, legal settlement, and fines. Telecommunication operators or other companies involved in cybersecurity cases are actively examined by regulatory authorities like the Federal Trade Commission (FTC) and the Federal communications Commission (FCC).

In the table below, a summary of telecom data breach incidents and enforcement measures witnessed in North America are displayed.

Table 3.

Telecom Data Breaches and Regulatory Responses in North America

Country	Year	Nature of Data Breach	Telecom Company	Regulatory Action	Fine Imposed
USA	2023	T-Mobile subscriber data breach (~40 million users)	T-Mobile	FTC settlement	$350 million
USA	2022	AT&T mobile data leak	AT&T	FCC fine & audit	$25 million
Canada	2021	Rogers data breach (~1.5 million users)	Rogers	Privacy Commissioner investigation	No fine

Source: Reuters (2023, 2025b); Federal Communications Commission (2024); T-Mobile Data Breach Settlement. (2023).

Table 3 shows the telecom data breaches and regulatory responses in North America. As analysed, regulatory enforcement in the region is based on the legal settlements, regulatory investigations and compliance control.

Telecom companies that have been involved with data breaches have been known to pay substantial financial settlements (in the US) and they are also investigated by regulatory agencies. For instance, the T-Mobile data breach that affected millions of subscribers attracted a huge fine to the regulatory authorities T-Mobile Data Breach Settlement. (2023). Similarly, AT&T was subject to regulatory and financial penalties for failure to disclose customer data (Federal Communications Commission, 2024).

Canadian regulatory actions are more inclined to be investigative and corrective rather than huge financial penalties. This is a combined enforcement system of legal, regulatory and consumer protection in response to telecommunication cyber security crimes (Reuters, (2023).

Telecom Data Breaches in Africa

The enforcement of telecom data protection in the African markets differs greatly according to the regulatory capabilities as well as the legal frameworks of the respective countries. Whereas there are examples of countries that have enforced severe fines in case of violation of regulations, other nations have had to depend more on inquiries and compliance checks. The table below lists some of telecom data breach and regulatory reactions in the African telecom markets.

Table 4.

Telecom Data Breaches and Regulatory Responses in Selected African Countries

Country	Year	Nature of Breach	Telecom Company	Regulatory Action	Fine Imposed
South Africa	2020	Customer data breach	MTN	Investigation by Information Regulator	Not disclosed
Kenya	2021	Subscriber data security issue	Safaricom	Regulatory warning	No fine

Source: Reuters (2024); GSMA Intelligence Africa Report (2023); ITU Telecom Reports (2022).

Table 4 provides an overview of selected cases of telecom data breaches and regulatory interventions in African telecom markets. The results suggest that the regulatory enforcement practices differ between countries, depending on the legal and

institutional frameworks, as well as the level of development of the data protection regimes. The regulators have taken enforcement action by conducting investigations, compliance reviews, and monitoring procedures, instead of issuing significant monetary penalties in several instances.

The analysis indicates that African telecom markets adopt diverse regulatory approaches, ranging from advisory and corrective measures to more formal enforcement actions. These differences reflect variations in institutional capacity, regulatory maturity, and the development of data protection frameworks across the continent. The findings highlight the need to strengthen regulatory institutions in order to improve cybersecurity oversight and enhance the protection of subscriber data.

Overall, the evidence suggests that the effectiveness of telecom data protection measures varies across African jurisdictions due to differences in enforcement capacity, regulatory maturity, and institutional development (GSMA Intelligence, 2024; ITU, 2022).

India Context – PSU vs Private Telecom Companies

India is an interesting example to study regulatory responses to telecom data breaches since both the public and private telecom operators are regulated by the same authority. The comparison of regulatory measures in these categories would be useful in explaining the type of enforcement embraced by telecom regulators.

The data presented in the table below compares the chosen data security incidents of the public sector undertakings (PSUs) and the cases with the private telecom companies in India.

Table 5.

India Context – PSU vs Private Telecom Companies

Type	Telecom Company	Year	Nature of Breach	Regulatory Action	Fine Imposed
PSU	BSNL	2025	Subscriber data exposure	No action	No fine
PSU	MTNL	2024	Customer data issue	Advisory	No fine

PSU	RailTel	2022	Cybersecurity incident	Internal audit	No fine
Private	Bharti Airtel	2024	KYC & mobile data leak	Advisory	No fine
Private	Reliance Jio	2023	Third-party access	Clarification	No fine
Private	Vodafone Idea	2023–24	SIM & KYC lapses	Notice	No fine

Source: Business Standard (2024); The Economic Times (2023 & 2024); PRS Legislative Research (2023)

A comparative summary of telecom data breaches in PSUs and the commercial telecom operator in India is given in Table 5. The table shows the response taken by the regulatory bodies to case of data breach in the telecom sector to various ownership structures.

The fact that has been established is that regulatory actions in India have mostly been non-punitive irrespective of whether the telecom operator is a state-run organization or a privately-owned company. Most of the regulatory measures in the case of public sector enterprises like BSNL, MTNL, and RailTel Corporation have been in the form of advisory notices, internal audits or reviews of compliance. No financial fines were paid by such operators even in the instances of exposure of subscriber data or cybersecurity breaches reported.

The same regulatory trend is seen in terms of the private telecom companies such as Bharti Airtel, Reliance Jio as well as Vodafone Idea. Although regulatory authorities issued clarifications, notices, or advisory communications when reported problems in the field of data security, the cases did not result in financial fines. This implies that the regulatory strategy in respect to telecom data breaches in India is more compliance-based and less enforcement based.

The analysis of the PSU and private telecom companies shows that the ownership structure does not play a major role in the regulatory reaction to data security breaches. Rather, the regulators seem to focus on remedial action and enhancement of internal compliance, rather than on imposing financial fines. Even though such a practice may help to achieve cooperative compliance, the absence of potent punitive actions may weaken deterrence and diminish the motivations of telecom operators to increase the level of cybersecurity in the governance and data protection processes.

Overall, when comparing the telecom data breaches in Asia, Europe, North America, and Africa, it is clear that there are major variations in the way the regulatory enforcement process occurs. The approach used by European regulators is more deterrence based with serious monetary fines as per GDPR, as compared to North America where settlements and regulatory reviews are used. Most Asian markets like India, on the other hand, are advisory and compliance responders. There is an ambivalent practice of enforcement in African telecom markets which is based on the ability to control.

Result and Discussion

This part is the comprehensive discussion of the telecommunication data breaches in Asia, Europe, North America and Africa and the amalgamation of the analysis of Tables 1-5. The findings reveal the geographical differences in enforcement of regulations and control based on ownership, with or without monetary and non-monetary punishments.

In Asia, the enforcement of regulations is relatively non-punitive. In India, most of the breaches (BSNL, Bharti Airtel, Reliance Jio, Vodafone Idea, MTNL, RailTel Corporation) were resolved by issuing an advisory notice, clarifying doubts, doing an internal audit or a compliance audit and no penalties were imposed (see Table 1). This is also true for Sri Lanka and Nepal, as they issued the warning or notices and the Chinese undertook compliance audits without mentioning the fines. In contrast, in South Korea, SK Telecom was fined USD 96.53 million in 2025 for breaching data of 27 million subscribers. These developments show that while some of the Asian regulators are beginning to take more proactive approach to enforcement actions, the deterrent effect is still limited, particularly in the case of advisory actions.

The more detailed data of the regulatory regime in India (Table 5) of the PSUs vis-à-vis the case of the private telecom operators shows that ownership makes little difference in the regulatory practices. Advisory and internal audit was given to the operators of the public sector (such as BSNL, MTNL and RailTel Corporation) and some more active supervision in the operators of the private sector (such as Bharti Airtel, Reliance Jio and Vodafone Idea). However, there were no financial penalties to either. This is empirical evidence of a pervasive non-financial regulation and a possible gap in deterrence in PSU and in private sector.

In Europe, enforcement under the General Data Protection Regulation (GDPR) is consistent, predictable, and strongly deterrence-oriented (Table 2). Telecom operators in the United Kingdom, Italy, Spain, and Germany have been subjected to substantial monetary penalties for violations involving customer and subscriber data. For example, Telecom Italia (TIM) was fined €27.8 million, Vodafone Spain €8.15 million, Deutsche Telekom €17 million, and BT Group £1.1 million. These penalties demonstrate the strong deterrence-based regulatory model adopted across Europe, where accountability and proactive compliance are strongly encouraged. The findings suggest that the certainty and severity of sanctions under the GDPR have strengthened organizational commitment toward cybersecurity governance and data protection compliance.

The enforcement paradigm that is evident in North America (Table 3) is a hybrid, and involves financial settlements, compliance audit and legal scrutiny. In the U.S. T-Mobile 2023 (40 million users) caused the company to pay USD 350 million to the FTC in settlement and AT&T was fined USD 25 million of FCC and compliance audits. The Canadian Privacy Commissioner opened an investigation but didn't fine Rogers 2021 breach. This model suggests that we need to focus on the settlement- and compliance-based model that will create deterrent and accountability, but not regular fines.

Regulatory approaches vary across African telecom markets depending on institutional capacity, legal frameworks, and the maturity of data protection regimes (Table 4). The cases examined in this study indicate that regulatory responses have generally focused on investigations, compliance reviews, and supervisory oversight rather than the imposition of substantial monetary penalties. This suggests that enforcement practices differ across jurisdictions, reflecting variations in regulatory capacity and institutional development. The findings further indicate that strengthening regulatory institutions and data protection frameworks is important for improving cybersecurity governance and enhancing the protection of subscriber data across African telecom markets.

Cross-regional comparison highlights four distinct enforcement philosophies:

1. Asia – Primarily advisory and corrective, with limited fines; enforcement capacity varies across countries.
2. Europe – Consistent, rule-based, and monetary-focused; substantial fines enhance deterrence.
3. North America – Settlement- and oversight-driven; combines financial and compliance measures for accountability.

4. Africa – Mixed enforcement approaches reflecting differences in regulatory maturity and institutional capacity.

Table 6.

Cross-Continental Comparison of Regulatory Philosophies, Penalty Severity, and Enforcement Approaches in the Telecom Sector

Region	Enforcement Philosophy	Penalty Severity	Key Regulatory Approach
Asia	Compliance-based	Low to Moderate	Advisories, audits, notices
Europe	Deterrence-based	High	GDPR monetary penalties
North America	Settlement-based	High	Settlements and investigations
Africa	Mixed approach	Variable	Investigations, compliance monitoring and warnings

Source: Compiled by the Author based on Tables 1–5.

Table 6 provides a unified cross-continental comparison of regulatory enforcement philosophies, penalty severity, and regulatory approaches in the telecommunications sector. The findings are broadly consistent with Becker's Deterrence Theory (1968), which suggests that compliance is more likely when sanctions are certain, severe, and predictable. European regulators demonstrate the strongest deterrence-based approach through the imposition of substantial monetary penalties under the General Data Protection Regulation (GDPR). In North America, enforcement is primarily driven by regulatory settlements, investigations, and compliance oversight. In contrast, most Asian jurisdictions continue to rely on advisory notices, audits, and corrective measures, although South Korea represents an important exception through the use of significant financial penalties. These variations indicate that regulatory philosophy plays an important role in influencing corporate cybersecurity behaviour and data protection compliance.

An important finding emerges from the comparison between public and private telecom operators in India (Table 5). The analysis indicates that regulatory responses remain largely compliance-oriented regardless of ownership structure. Public sector operators such as BSNL, MTNL, and RailTel, as well as private operators including Bharti Airtel, Reliance Jio, and Vodafone Idea, have generally been subjected to advisories, notices, clarifications, or internal audits rather than financial penalties.

While such measures may support corrective compliance and operational improvements, the absence of substantial monetary sanctions may reduce the deterrent effect of regulation and weaken incentives for proactive investment in cybersecurity infrastructure, data governance, and subscriber data protection.

African telecom markets exhibit a mixed pattern of regulatory enforcement. While some jurisdictions have adopted more formal enforcement mechanisms, others continue to rely primarily on investigations, warnings, and compliance monitoring. These differences reflect variations in institutional capacity, regulatory maturity, and the development of data protection frameworks across countries. Consequently, African telecom markets represent a transitional regulatory environment in which enforcement approaches range from deterrence-based actions to compliance-oriented oversight.

Overall, the comparative analysis demonstrates that regulatory frameworks, enforcement intensity, and penalty structures significantly influence telecom data protection outcomes across regions. Differences in legal provisions, institutional capacity, and enforcement philosophies contribute to variations in regulatory effectiveness. The findings suggest that stronger and more consistent enforcement mechanisms are associated with higher levels of accountability and cybersecurity preparedness among telecom operators. Therefore, policymakers and regulators should focus on developing balanced regulatory systems that combine effective enforcement with compliance support in order to strengthen the protection of subscriber data and enhance trust in digital telecommunications infrastructure.

Reasons Behind Differential Imposition of Fines for Telecom Data Breaches: India versus International Jurisdictions

Differences in Legal Frameworks and Penalty Provisions

There were no pre-existing and enforceable laws concerning data protection in India during the period in which most telecom data breaches occurred, which is among the key factors to explain this phenomenon of small fines in the country. Until a new law, the Digital Personal Data Protection Act (DPDP Act), 2023, India depended mostly on the Information Technology Act, 2000, and the telecommunication specific laws, which had no specific and strict penalty provisions of a gross breach of personal data.

In terms of what we see in the European Union the main legislation is the European Union General Data Protection Regulation (GDPR) which is the framework

that gives regulators the power to issue very clear legal authority to fine companies up to 4% of the global annual turnover. This has enabled European governments to impose what in some cases are very large penalties on telecommunication companies like Vodafone Spain, Deutsche Telekom, and Telecom Italia as reported by Reuters (2021, 2022). Also, in South Korea we see the Personal Information Protection Act (PIPA) which gives the government special authority to do out large scale penalties, for instance in the largest fine in the country's history which was issued to SK Telecom after a large-scale personal data leak affecting millions of users (Reuters, 2025a).

Regulatory Capacity and Enforcement Philosophy

In India telecom regulation is a compliance issue as opposed to being punitive. The Telecom regulatory body is a government entity which is mainly in an advisory role and enforcement is done by other agencies which do not have a very strong arm and hence the enforcement processes are slow (PRS Legislative Research, 2023; The Economic Times, 2024). In India, regulatory responses to telecom data breach incidents have largely focused on internal investigations, compliance monitoring, and advisory measures rather than the imposition of significant monetary penalties.

In Europe and North America on the other hand, regulators have a deterrent-based enforcement philosophy. Consolidated powers of investigation and enforcement Regulatory authorities including the Information Commissioner of the UK (ICO), the Data Protection Authority of Italy (Garante), the US Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) have combined investigative and enforcement powers. The news sources suggest that such agencies often impose hefty fines and legally enforce settlements to denote regulatory severity as has been the case with T-Mobile and AT&T in the U.S. (Reuters, 2022; 2023).

Ownership Structure and Political Economy Considerations

The ownership structure is equally important in assessing the possible outcomes in India. The two main players in the market, BSNL and MTNL, are public sector undertakings (PSUs) which are owned by the central and state governments of India respectively. Imposing heavy fines on them will simply shift the burden on the government. Reports in the Indian media suggest that instead of imposing heavy penalties the regulator is left with little option but to resort to non-monetary measures and indirectly bring the government to book (The Economic Times, 2023; Business Standard, 2024).

In the global industry large telecom operators are mostly privately owned. They compete hard for market share and therefore when regulators impose fines on companies like T-Mobile, Vodafone and Deutsche Telekom, they don't come across as a social cost to consumers but as a corporate cost. Financial Times (2018) reports that in this environment, EU regulators can be more tough without much of a pushback from politicians.

Institutional Emphasis on Consumer Protection and Transparency

Indian regulations following huge telecom data breach were more about ensuring continuity to subscribers and smoothness of operations than about compensation to affected consumers or imposing a penalty on the defaulters. India did not have a provision for breach notification until recently and as a result, data breach incidents largely remained under the wraps until the recent telecom data breach, which grabbed all the media attention.

Compared to global policies, which focus on increased transparency and consumer rights, breaches in the country can have much more severe outcomes. In Europe and the US, such incidents are required by law to be publicly disclosed, which often leads to data breach investigations by regulatory bodies, consumer class-action lawsuits, and a substantial amount of negative publicity and damage to a company's brand. Reuters (2023) reported on several instances of large-scale telecom data breaches in the US and EU, and the ways in which the public disclosure requirement and class-action lawsuits have prompted regulators to levy hefty fines on the involved companies.

Stage of Regulatory Maturity and Policy Evolution

The difference in the ability to enforce fines also underlines the differences in levels of maturity between the data protection regimes in Europe/North America and India. Enforcement of data protection in Europe/North America is a mature process that has evolved over several decades, backed by a high level of institutional capability and judicial support. In contrast, India is still in a transition phase in terms of data governance and the recently enacted Digital Personal Data Protection Act, 2023 (DPDP Act, 2023) is a significant policy shift that will introduce a significantly stricter approach to levying penalties. Initial news reports indicate that the long-term impact of the ability to enforce penalties in the highly competitive Indian telecom market has yet to be felt (Financial Express, 2025; Reuters, 2023).

There is a huge gap in dealing with telecom data breaches in India vis-à-vis the global best practices. Countries like South Korea, US, UK, and Italy have imposed huge penalties for data breaches (Reuters, 2023), whereas in India punishments are only advisory in nature. It is a case of less strong provisions of historical law, divided enforcement, PSU ownership issues and a compliance-focused regulation. However, the study findings suggest that a more deterrence-oriented enforcement system would be appropriate to ensure that the current telecom data protection regime in India is on par with the global best practices.

From the perspective of Becker's deterrence theory (1968), the Digital Personal Data Protection Act (DPDP Act), 2023 is expected to significantly influence corporate cybersecurity behaviour in India. Becker argued that organizations are more likely to comply with regulations when the expected cost of violations exceeds the potential benefits of non-compliance. With the introduction of substantial financial penalties under the DPDP Act, telecom operators may increase investments in cybersecurity infrastructure, employee training, data governance systems, and breach prevention mechanisms. Therefore, the DPDP Act has the potential to shift India's telecom sector from a largely compliance-oriented regulatory environment toward a stronger deterrence-based framework, similar to those observed in Europe and other advanced jurisdictions.

Conclusion

This paper focuses on telecom breaches and the regulations thereof in various regions of the world. Using a comparative analysis of breaches and related enforcement actions in Asia, Europe, North America and select African markets, the paper notes striking differences between countries and regions with respect to cybersecurity incident enforcement in the telecom sector, as evidenced by the various tables delineating enforcement actions and regulations in respective jurisdictions.

The responses clearly indicated that there were distinct regional nuances in how regulations are enforced. In European countries, the enforcement under General Data Protection Regulation (GDPR) is primarily deterrence driven where the fines are huge to ensure that organizations are proactive in data protection. In North America, the responses ranged across multiple disciplines and indicated that there was a need for regulation to be backed by financial settlements, regular surveillance and audits to ensure telecom organizations are compliant with data protection regulations. In most of the Asian telecommunication markets, the responses

indicated that there was minimal need for fines as advisories, compliance checks, internal investigations etc. were sufficient. There was a variation in the responses from African telecom markets based on the level of maturity and capacity of the regulatory bodies.

This paper provides a comprehensive analysis of the Indian telecom market on comparison between public sector players and private telecom players. The report identifies a significant gap in the existing regulatory framework. While regulatory bodies make announcements, warnings and specify compliances, the absence of financial fines on non-compliance may limit the impact of their initiatives and will encourage telecom players to take cybersecurity management and data security lightly.

Research globally has highlighted the need for strengthened legal frameworks, clearer penalties and consistent enforcement to protect telecom data. As digital connectivity continues to grow, regulators will need to enhance their capacity to deter those who would misuse telecom data and to protect the sensitive information of subscribers to preserve public trust in critical communications infrastructure.

Furthermore, the implementation of the Digital Personal Data Protection Act, 2023 may further strengthen India's enforcement capacity and encourage a more deterrence-oriented approach to telecom data protection.

References

Acquisti, A., Taylor, C. R., & Wagman, L. (2016). *The economics of privacy*. *Journal of Economic Literature, 54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265–300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12

Becker, G. S. (1968). *Crime and punishment: An economic approach*. *Journal of Political Economy, 76*(2), 169–217. https://doi.org/10.1086/259394

BharatNet. (2024). *BharatNet Project*. Retrieved December 20, 2025, from https://usof.gov.in/en/bharatnet-project

Böhme, R., & Moore, T. (2012). *The economics of information security investment*. *Journal of Information Security, 3*(2), 75–83. https://doi.org/10.4236/jis.2012.32010

Böhme, R., Laube, S., & Riek, M. (2019). *A fundamental approach to cyber risk analysis*. Variance, 12(2), 161–185 https://doi.org/10.66573/001c.120742

Business Standard. (2024, June 26). *BSNL data breach exposes 278 GB of sensitive telecom info, twice in 6 mts*. Retrieved December 20, 2025, from https://www.business-standard.com/companies/news/bsnl-data-breach-exposes-278-gb-of-sensitive-telecom-info-twice-in-6-mts-124062600314_1.html

Creemers, R. (2022). *China's emerging data protection framework*. Journal of Cybersecurity, 8(1), tyac011. https://doi.org/10.1093/cybsec/tyac011

ETTelecom. (2024). *BSNL data breach highlights weak cybersecurity enforcement in India*. https://telecom.economictimes.indiatimes.com/

ETTelecom. (2025). *SK Telecom cyberattack exposes subscriber data*. https://telecom.economictimes.indiatimes.com/

European Data Protection Board. (2024). *EDPB Annual Report 2023*. Retrieved December 10, 2025, from https://www.edpb.europa.eu/our-work-tools/our-documents/annual-report/edpb-annual-report-2023_en

Federal Communications Commission. (2024, September 17). *FCC Announces $13 Million Settlement with AT&T Resolving Vendor Cloud Breach Investigation*. Retrieved December 10, 2025, from https://www.fcc.gov/document/fcc-settles-att-vendor-cloud-breach

Financial Express. (2025, September 27). *DPDP Act needs to have broader approach*. Retrieved January 10, 2026, from https://www.financialexpress.com/life/technology-dpdp-act-needs-to-have-broader-approach-3991224

Financial Times. (2018, May 23). *GDPR: Europe takes lead*. Retrieved December 10, 2025, from https://www.ft.com/content/bd3eb2ae-5ea0-11e8-9334-2218e7146b04

Gal-Or, E., Gal-Or, R., & Penmetsa, N. (2018). *The Role of User Privacy Concerns in Shaping Competition Among Platforms*. Information Systems Research, 29(3), 698–722. https://doi.org/10.1287/isre.2017.0730

Gao, L., Chen, Z., Zhao, W., & Lai, X. (2025). *Does cybersecurity regulation reduce corporate data-breach risk? Finance Research Letters, 78*, 107171. https://doi.org/10.1016/j.frl.2025.107171

Greenleaf, G. (2021). *Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance*. Privacy Laws & Business International Report, 169, 10–13 http://dx.doi.org/10.2139/ssrn.3836348

Greenstein, S., & Prince, J. (2006). *The diffusion of the Internet and the geography of the digital divide in the United States* (NBER Working Paper No. 12182). National Bureau of Economic Research. https://doi.org/10.3386/w12182

GSMA Intelligence. (2023). *The Mobile Economy Sub-Saharan Africa 2023*. Retrieved January 10, 2026, from https://www.gsmaintelligence.com/research/the-mobile-economy-sub-saharan-africa-2023

GSMA Intelligence. (2024). *Trusted data and insights for the global mobile ecosystem*. Retrieved January 10, 2026, from https://www.gsmaintelligence.com/

HT Digital Streams Ltd. (2024, July 5). Bharti Airtel denies data breach of 37.5 crore subscribers. Retrieved January 10, 2026, from https://www.livemint.com/companies/news/bharti-airtel-data-leak-telecom-major-denies-security-breach-of-over-37-crore-customers-after-hackers-post-allegations-11720173165182.html

Information Commissioner's Office (ICO). (2024). *Annual Report 2023–24*. Retrieved January 10, 2026, from https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf

International Telecommunication Union (ITU). (2022). Global Cybersecurity Index 2020. Retrieved December 10, 2025, from https://www.itu.int/pub/D-STR-GCI.01-2021

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). *Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kuner, C. (2022). *The GDPR: A transnational perspective*. *International Data Privacy Law, 12*(1), 3–15. https://doi.org/10.1093/idpl/ipab042

PRS Legislative Research. (2023). *The Digital Personal Data Protection Bill, 2023*. Retrieved January 10, 2026, from https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

Reuters. (2021). European regulators fine telecom firms under GDPR rules. Retrieved December 10, 2025, from https://www.reuters.com

Reuters. (2022, January 21). *Cybersecurity and data privacy foresight 2022*. Retrieved December 10, 2025, from https://www.reuters.com/legal/legalindustry/cybersecurity-data-privacy-foresight-2022-2022-01-21/

Reuters. (2023, October 16). *Your organization has suffered a data incident: Now here are the regulators it will face.* Retrieved January 10, 2026, from https://www.reuters.com/legal/legalindustry/your-organization-has-suffered-data-incident-now-here-are-regulators-it-will-2023-10-16/

Reuters. (2024, November 13). *China-linked hackers stole surveillance data from telecom companies, U.S. says*. Retrieved December 10, 2025, from https://www.reuters.com/technology/cybersecurity/china-affiliated-actors-compromised-networks-multiple-telecom-companies-us-says-2024-11-13/

Reuters. (2025a). *South Korea agency fines SK Telecom $97 million over major data leak*. https://www.reuters.com/sustainability/boards-policy-regulation/south-korea-agency-fines-sk-telecom-97-million-over-major-data-leak-2025-08-28/

Reuters. (2025b, February 1). *Data Privacy and Cybersecurity: 2024 Trends and Developments*. Retrieved January 10, 2026, from https://www.reuters.com/practical-law-the-journal/transactional/data-privacy-cybersecurity-2024-trends-developments-2025-02-01/

Romanosky, S. (2016). *Examining the costs and causes of cyber incidents*. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Romanosky, S., Telang, R., & Acquisti, A. (2011). *Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management, 30*(2), 256–286. https://doi.org/10.1002/pam.20567

TeleGeography. (2024). *State of the Network 2024.* Retrieved January 10, 2026, from https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2024.pdf

Termly. (2026). *61 Biggest GDPR Fines & Penalties So Far [2026 Update]*. Retrieved March 2, 2026, from https://termly.io/resources/articles/biggest-gdpr-fines/

The Economic Times. (2023, August 18). *Government will ensure orderly transition to new data rules: MoS IT Rajeev Chandrasekhar.* Retrieved December 10, 2025, from https://economictimes.indiatimes.com/tech/technology/government-will-ensure-orderly-transition-to-new-data-rules-mos-it-rajeev-chandrasekhar/articleshow/102811046.cms

The Economic Times. (2025, June 30). *Trai's new proposal may help check spam as it complements data protection laws*. Retrieved December 10, 2025, from https://economictimes.indiatimes.com/tech/technology/trais-new-proposal-may-help-check-spam-as-it-complements-data-protection-laws/articleshow/122146683.cms

Times of India. (2023, August 3). Entities violating digital data protection norms to face penalty of up to Rs 250 crore: DPDP 2023. Retrieved December 10, 2025, from https://timesofindia.indiatimes.com/india/entities-violating-digital-data-protection-norms-to-face-penalty-of-up-to-rs-250-crore-dpdp-2023/articleshow/102392400.cms

Times of India. (2024, June 26). *Hacker claims to have critical security data, SIM card details of BSNL customers*. Retrieved January 10, 2026, from https://timesofindia.indiatimes.com/technology/tech-news/hacker-claims-to-have-critical-security-data-sim-card-details-of-bsnl-customers/articleshow/111289752.cms

T-Mobile Data Breach Settlement. (2023). *T-Mobile Data Breach Settlement*. Retrieved December 10, 2025, from https://www.t-mobilesettlement.com/

Wolters, P. T. J. (2019). *The enforcement by the data subject under the GDPR*. *Journal of Internet Law, 22*(8), 22–31. Retrieved January 10, 2026, from https://repository.ubn.ru.nl/handle/2066/200981