4.4 Numerical Data Analysis

The present section is a detailed quantitative analysis of how far the effectiveness of biometric data privacy laws in UK and India has been proper. Its analysis is based on key data points regarding biometric data breaches, compliance rates, and enforcement actions obtained from annual reports of (ICO, 2019-2024 and .

4.4.1 Biometric Data Breaches

- **United Kingdom:** According to the ICO's Annual Reports for the years 2020-2021, cases of reported breaches of biometric data increased by 27%. The reported breaches, which were 120 in 2018, increased to 150 in 2019, 190 in 2020, 240 in 2021, and then 300 in the year 2022. This steady increase reflects the growing adoption of biometric technologies in sectors such as finance, healthcare, and law enforcement. Despite these strict regulations, the rising rate of breaches under the GDPR suggests that organizations are struggling to implement effective security measures.

  Analysis: The ICO has fined a total sum of £50 million from 2018 to 2021 due to non-compliance with GDPR stipulations. The fact that such fines have been issued certainly demonstrates its proactivity in matters of enforcement. However, the increased number of breaches somewhat vindicates the perception that financial penalties do not suffice to act as a deterrent to non-compliance. Other measures should be taken—such as increasing audits or providing more support to organizations during the implementation of security protocols.

• **India:** In a 2021 (CIS) report, revealed that during the period from 2018 to 2020, nearly 135 million Aadhaar numbers have been compromised via data breaches. These breaches stand to underscore the vulnerabilities of India's biometric data infrastructure and, more critically, the lack of proper security measures stipulated in the Aadhaar Act. This is further compounded by the lack of stiff enforcement mechanisms for cases of breaches, which have largely gone unpunished.

Analysis: Unlike in the UK, where fines actually deter such offences, offences and breaches occur with very little consequence in India. It is in this numerical data that there exists the need to push for improved legal protections and enforcement mechanisms, particularly in view of the pending PDPB.

4.4.2 Data Protection Complaints in the UK (2018-2023)

The UK's Information Commissioner's Office (ICO) has seen significant activity in processing data protection complaints since the enforcement of the General Data Protection Regulation (GDPR) in 2018. Between 2019 and 2023, the number of complaints filed with the ICO fluctuated, revealing public engagement with data protection issues as well as organizational struggles to maintain GDPR compliance.

- **2019/20**: 39,000 complaints received.
- **2020/21**: 36,343 complaints received.
- **2021/22**: 33,753 complaints received.
- **2022/23**: 39,721 complaints received.
- **2023/24**: 41,500 complaints received.

4.4.2.1 Trend Analysis

New complaint data from ICO reveals that from the year 2019 to 2024, ICO had a decrease in complaints immediately after the implementation of GDPR and then observe a year of transition where the organization took time to violate the GDPR regulation. But, the increase of complains from the year 2021, depicts continuing public consciousness and the issue of stringency that arises from following the rules, particularly when implementing the new technologies and practices referring to the biometric data. It is also observed that the rise in complaint has pointed out the fact that ICO enforcements have driven people more towards reporting possible breaches.

4.4.2.2 Key Insight

The changes in the level of complaints are indicative of the changes that occur in data protection in the UK. While many organizations have enhanced compliance it is evident that the number of complaints is still on the rise meaning that some sectors in particular those that use biometric data still pose serious problems. People have also been made aware of their data rights under the General Data Protection Regulation hence pushing up the complaints.

4.5 Enforcement Actions: Monetary Penalties in the UK (2018-2023)

The ICO has ensured that the non- compliance of GDPR regulation is punished with strong measures. Such penalties have increased over the years with more indication of an enforcement that is likely to be preemptive rather than reactive in cases of severe violations.

- **2019/20**: £1.3 million in penalties.
- **2020/21**: £3.5 million in penalties.
- **2021/22**: £5.2 million in penalties.

- **2022/23**: £6.3 million in penalties.
- **2023/24**: £7.0 million in penalties.

4.5.1 Trend Analysis

The continual rise in penalties demonstrates ICO's commitment towards the protection of personal data especially where biometric data is involved. Penalties have increased over time and it also reveals that it has not been easy for organisations to implement GDPR in its entirety. Main attention should be paid to healthcare, finance, and retail companies, as such breaches led the ICO to raise fines and make companies complied with regulations.

4.5.2 Key Insight

The increase of fines shows the ICO commitment to enforcing GDPR and protecting biometric data. However, an upward trend in the fine also suggests that more organizations are not serious with security even in the face of these fines to safeguard their clients' information.

4.6 Compliance Rates with GDPR in the UK (2018-2023)

Exploration of the extent to which organisations in the United Kingdom have complied with general data protection regulation (GDPR) since implementation have revealed a trend in the enhancement of the compliance level. A lot of organisations have endeavored to meet the stringent measures of GDPR resulting to high compliance levels.

- **2019/20**: 82% compliance rate.
- **2020/21**: 85% compliance rate.
- **2021/22**: 87% compliance rate.
- **2022/23**: 90% compliance rate.
- **2023/24**: 92% compliance rate.

4.6.1 Trend Analysis

The relative increase in the GDPR compliance rates indicates that the organizations are getting to understand the need to protect biometric and other sensitive data. Nevertheless, some issues persist especially in the fields that require the precise and accurate identification of the biometric data including law enforcement agencies together with financial institutions.

4.6.2 Key Insight

The steady increase in compliance rates was a clear indication that organizations are more conscious of the need of protecting personal and biometric data. However, the growing number of complaints and penalties even point to the fact that many organizations including small enterprises may be having a hard time implementing the measures provided under GDPR.

4.7 Outcome Decisions by ICO in the UK (2018-2023)

The number of cases handled and the number of outcome decisions may vary, but the ICO's efficiency in dealing with a case and its capacity to come up with solutions has remained stable.

- **2019/20**: 39,724 decisions.
- **2020/21**: 39,332 decisions.
- **2021/22**: 37,342 decisions.
- **2022/23**: 35,332 decisions.
- **2023/24**: 33,000 decisions.

4.7.1 Trend Analysis

This slight decrease in the number of outcome decisions suggests that the ICO might be increasingly focusing on the more complex cases, which involve breaches of biometric data and therefore take longer to resolve. The ICO does appear resolute in its capability to manage and conclude complaints amidst challenges that keep popping up from evolving laws and practices in data protection.

4.7.2 Key Insight

While the ICO has been able to process these cases efficiently, a decline in outcome decisions suggests that more complex cases could be emerging with the increased expansion of biometric data use. Many such applications are also enveloped in serious investigations and enforcement activities, particularly in high-risk sectors.

4..8 Biometric Data Protection in India

4.8.1 Aadhaar Enrolment and Growth (2018-2023)

UIDAI has been implementing the Aadhaar project continuously since its inception. From 2018 through 2023, Aadhaar enrollment took place exponentially, entrenching Aadhaar as a critical utility for identity verification and service delivery.

- **2018-19**: 123.57 crore Aadhaar numbers generated.
- **2019-20**: 125.79 crore Aadhaar numbers generated.
- **2020-21**: 129.04 crore Aadhaar numbers generated.
- **2021-22**: 132.96 crore Aadhaar numbers generated.
- **2022-23**: 136.65 crore Aadhaar numbers generated.

4.8.1.1 Trend Analysis

The continuous growth in the enrolment of Aadhaar is a testament to the efforts of the Indian government to provide all the residents of the country with a unique identification number. Considering the many challenges on issues related to privacy and security of data, Aadhaar has grown to achieve near-universal coverage and has been playing a crucial role in facilitating access to social welfare programs, financial services, and subsidies.

4.8.1.2 Key Insight

Aadhaar's widespread simply points to its importance within the India nation's digital framework. However, concerns about privacy and security of data remain challenging, in particular with the Supreme Court ruling that limits its use to certain purposes.

4.8.2 Aadhaar Authentication Transactions (2018-2023)

Aadhaar usage for authentication has also shaped up so well over the years, which makes its case very strong for identity verification.

- **2018-19**: 1,080.47 crore authentication transactions.
- **2019-20**: 1,113.54 crore authentication transactions.
- **2020-21**: 1,413.40 crore authentication transactions.
- **2021-22**: 1,771.00 crore authentication transactions.
- **2022-23**: 2,291.97 crore authentication transactions.

4.8.2.1Trend Analysis

This steady growth of authentication transactions testifies to the fact that Aadhaar is gradually gaining momentum in verification of identities across sectors, from banking to health. The increasing number of transactions signifies that Aadhaar has indeed become an indispensable tool for service delivery in India.

4.8.2.2 Key Insight

As Aadhaar has been successful in making life easier for millions of Indians by allowing seamless identity verification, the importance of its contribution to bringing in more transparency and weeding out fraud from government programs cannot be emphasized enough. At the same time, its application on this scale raises many questions pertaining to data privacy and misuse of personal information.

4.8.3 Data Protection and Privacy Measures in Aadhaar

UIDAI has been taking drastic measures towards keeping Aadhaar data safe while ensuring that the issues of strong encryption, biometric locking mechanisms, and virtual IDs are taken care of. These measures have been suggested to ensure that the data on Aadhaar would remain well-protected and that the apprehension of the privacy advocates and the Supreme Court is met.

4.8.3.1 Key Insight

Despite use of security measures, concerns about the centralized nature of Aadhaar and potential breaches remain. While UIDAI has taken steps in enhancing data security, continuous vigil is needed so that Aadhaar data will remain protected, especially as its usage goes up across sectors.

4.9 Comparative Biometric Analysis and Key Differences

The comparison done on biometric data privacy in the UK and India shows a wide difference in the regulatory framework and enforcement. While the UK's GDPR is more focused on stringent data protection with robust enforcement, in the case of India's Aadhaar system, the basic operational purpose is to establish identity for service delivery, and the question of privacy is taken care of in bits and pieces.

- **Enforcement**: The UK's ICO is proactive in imposing penalties and enforcing compliance, while the UIDAI in India is more enrolment and authentication-oriented, with less enforcement related to breach of privacy.
- **Privacy Protections**: Individual rights and data protection are cardinal in the GDPR in the United Kingdom, while Aadhaar's legal framework has been assailed for lacking proper safeguards for privacy.

4.10 Compliance Rates

- **United Kingdom:** Compliance with DPIA rates in the UK is reported to be as high as 85% for large organizations but lower for SMEs, where only 65-70% of smaller businesses are conducting these assessments (ICO, 2023). This underlines the challenges faced by smaller organizations when working to implement resource-intensive requirements of the GDPR.

Analysis: Whereas large organizations broadly complied with the provisions of the GDPR, SMEs also struggle with the intricateness and costs associated with the protection of personal data. The work of the ICO in supporting smaller businesses with guidance has helped in increasing compliance, but certainly much more may be needed in terms of targeted interventions to ensure that all organizations are meeting their legal obligations. Compliance itself does seem to equate to effective data protection, as the number of breaches continues to rise despite high compliance rates.

India: Moreover, the share of Aadhaar-based authentication, as well as the general state of protection of personal data, still remains low, especially among private entities. According to Internet & Mobile Association of India (IAMAI) 2020, only 40% of organizations using Aadhaar-based authentication fully comply with the security requirements laid down by the Act. The lack of any regulatory oversight and mechanisms for effective enforcement was also to blame for such a poor level of compliance.

Analysis: The low compliance rate in India points to some deeper systemic issues in the Aadhaar framework. Numerically, therefore, it suggests that in the absence of better enforcement and clearer regulation, compliance would remain poor, while the security of biometric data continues to get more compromised. The pending PDPB might offer a fix for this problem by imposing stricter obligations on data processors and increasing regulatory oversight.

4.11 Enforcement Actions

- **United Kingdom:** While the ICO's enforcement actions show that the effort of the regulatory body in making the organization responsible, the increasing numbers of data breaches related to biometrics show that the fines will not be adequate to prevent the infringement. What may be required is a multi-faceted approach: proactive auditing, education for better understanding of the requirements of GDPR, and high-risk industries may require targeted interventions. The increase in fines, from £1.3 million in 2019/20 to £7.0 million in 2023/24, reflects both the increased focus of the ICO on strong enforcement and acts also as a barometer of the challenges organizations faced in achieving full implementation of GDPR-compliant measures (ICO, 203; ICO 2024).

Key Insight: The continuing escalation in fines and enforcement actions makes it clear that a state of regulatory vigilance is required. Clearly, the financial penal provisions serve to make an organization aware and sometimes act as deterrents; however, data shows that this needs to be supplemented with aftercare in the form of regular audits and more training programs, especially for smaller organizations.

- **India:** The lack of enforcement under the Aadhaar Act is a serious cause of concern. While the diffusion and use of the Aadhaar number-based biometric authentication have become all-pervasive, the enforcement against breaches or non-compliance by the organizations has been minimal. In fact, with no significant fines and sanctions, what has happened is the obtaining of minimum assurance that violations are passed over, and thereby the security of the data on biometrics is further compromised.

  Key Insight: The disparity between the UK and India in enforcement actions underscores the need for stronger regulatory oversight in India. The implementation of the Personal Data Protection Bill (PDPB) is critical for establishing a legal framework that enables UIDAI to enforce compliance and impose penalties. Without such a framework, the protection of biometric data will remain inadequate, and the risk of further breaches will persist.

4.12 Internet Penetration and Its Impact on Biometric Authentication in India

Internet penetration in India has rapidly increased, which has direct implications for the scalability and efficacy of Aadhaar authentication. Starting from a somewhat small base, the number of active internet users in India has grown sharply:

- **2018**: 560 million active internet users.
- **2020**: 622 million active internet users.
- **2022**: 759 million active internet users.

Analysis: Increased internet access, especially in rural areas, has enabled a majority of the population to access Aadhaar authentication facilities for government services, financial transactions, and subsidies through biometric verification. However, this digital spread also increases exposure to the dangers of breach and misuse of sensitive information because such measures are not followed sufficiently.

4.14 Growth in Digital Payments and Biometric Transactions

India has seen a dramatic rise in digital payments, many of which are linked to Aadhaar-enabled systems:

- **2022**: **46% of active internet users** in India engaged in digital payments.
- **Aadhaar Enabled Payment System (AEPS)**: By **March 2023**, AEPS transactions reached **1670.41 crore**, up from **0.50 crore in May 2014**.
- **BHIM Aadhaar Transactions**: Facilitated **5.66 crore transactions** in 2022, with **3.58 lakh merchants** utilizing Aadhaar authentication for digital payments.

Analysis: The rapid growth in digital payments, coupled with Aadhaar's authentication capabilities, reflects India's push for digital inclusion. However, the rise in transactions also raises concerns about the security of biometric data used for authentication in financial transactions. Strengthening the privacy protections surrounding biometric data in digital payments is essential to mitigate the risks of data breaches and fraud.

4.6 Barriers to Biometric Service Access in India

Despite the growth in internet usage, **50% of India's population remains non-active internet users**. The major reasons for not being able to access the internet are a lack of proper connectivity and awareness in rural areas

Analysis: These barriers widespread usage of Aadhaar in biometric services. Added to the inadequate infrastructure, low levels of digital literacy among citizens have compounded inability to avail full benefits of biometric identification systems-which limits the effectiveness of Aadhaar as a tool of inclusion. Such barriers need to be overcome if biometric services have to reach all cross-sections while data privacy is maintained.

4.7 Website Artifact Contribution

The interactive web portal developed as part of this research is a critical tool for visualizing and disseminating the findings from the comparative analysis. The portal enables users to engage with the data in an intuitive and accessible way, offering insights into the biometric data privacy frameworks in the UK and India through interactive features such as maps, timelines, and case studies.

4.7.1 Interactive Comparisons

Trendsetting functionalities of the web portal stand out in presenting side-by-side comparisons, through interactivity, of breaches of biometric data, compliance rates, and enforcement actions between the UK and India. Users can view the legal frameworks that set the two nations apart and glance backward through temporal trends to understand the tangible implications of these laws through data visualization.

For example, users can:

- Get access to the side-by-side comparison of the number of biometric data breaches reported every year in the UK and India.
- Access visual representations of compliance rates for a better idea of how GDPR compliance in the UK is gradually improving and the struggle of the Aadhaar framework in India.
- Review enforcement actions, with charts showing the monetary penalties issued by the ICO, against the lack of similar activity in India.

The interactive comparison of this information supports the accessibility of the data for researchers, policy makers, and legal professionals less familiar with the intricacies regarding biometric data privacy laws. This portal acts to educate users in exploring case studies that outline key legal decisions and corresponding implications upon biometric data protection.

4.7.2 Data Visualization and Accessibility

The web portal features a range of **data visualizations** created using R language for data analysis. According to Budianto 2020, these visualizations make it easier on users when trying to comprehend complex legal and statistical information. In reference to this, it will include the following.

- Line graphs in the trends over time of biometric data breaches: the user will have the capability to view the pattern and anomalies in it.
- Bar charts show the monetary fines issued by the ICO, representing the monetary consequences of compliance.
- Pie charts show the distribution of compliance rates across industries, which helps to identify those industries that are doing well in ensuring the adoption of GDPR-compliant practices and which ones are trailing.
- The portal makes this information in an interactive format, thus allowing users to work through the conclusions at their own pace and drill down into those areas most relevant to them.

Year	**Biometric Data Breaches**	**Data Protection Complaints Received**	**Compliance Rates (%)**	**Outcome Decisions**	**Monetary Penalties (millions GBP)**
2019/20	150	36,343	85	39,724	£3.5
2020/21	190	33,753	87	39,332	£5.2

Year	Biometric Data Breaches	Data Protection Complaints Received	Compliance Rates (%)	Outcome Decisions	Monetary Penalties (millions GBP)
2021/22	240	39,721	90	37,342	£6.3
2022/23	300	41,500	92	35,332	£7.0
2023/24	320	43,000	94	33,000	£7.5

Table1: United Kingdom: Biometric Data Breaches, Complaints, Compliance, and Outcome Decisions. (Sources ICO annual reports from 2019-2024)

This table shows the steady increase in **biometric data breaches** in the UK, rising from 150 in 2019/20 to 320 in 2023/24, alongside a significant rise in **monetary penalties**, which grew from £3.5 million to £7.5 million. Despite increasing **compliance rates** (85% to 94%), **data protection complaints** peaked at 43,000 in 2023/24, while **outcome decisions** by the ICO decreased over time, reflecting the growing complexity of cases.

Year	Digital Payments (% of Active Internet Users)	AEPS Transactions (crore)	BHIM Aadhaar Transactions (crore)
2018	36%	865.54	2.41
2019	40%	1,113.54	3.87
2020	42%	1,413.40	4.21
2021	44%	1,771.00	5.02

Year	Digital Payments (% of Active Internet Users)	AEPS Transactions (crore)	BHIM Aadhaar Transactions (crore)
2022	46%	2,291.97	5.66
2023	48%	2,500.00	6.10

Table 2: Growth in Digital Payments and Biometric Transactions (India) (sources AADHAR AR annual reports from 2020-2023)

This table provides the growth in digital payments as a percentage of active internet users, along with the Aadhaar Enabled Payment System (AEPS) and BHIM Aadhaar transactions in India from 2018 to 2023.

Year	Biometric Data Breaches	Compliance Rates (%)	Authentication Transactions (in Crore)
2019/20	N/A	40	1,113.54
2020/21	N/A	45	1,413.40
2021/22	N/A	50	1,771.00
2022/23	135M compromised	55	2,291.97

Table 3: India: Biometric Data Breaches and Authentication Transactions (Sources UIDAI AR 2019-2023)

This table highlights the increasing **compliance rates** in India, from 40% in 2019/20 to 55% in 2022/23, alongside a significant rise in **authentication transactions**, reaching 2,291.97 crore by

2022/23. However, biometric **data breaches** became a major concern in 2022/23, with 135 million records compromised, underscoring the need for stronger data protection.

Year	**Active Internet Users (millions)**	**Non-Active Internet Users (millions)**	**Aadhaar Authentication Transactions (crore)**
2018	560	540	1,080.47
2019	622	498	1,113.54
2020	700	472	1,413.40
2021	720	448	1,771.00
2022	759	380	2,291.97

Table 4: Biometric Authentication Transactions and Internet Access (India) (Sources IAMAI, AADHAR, annual reports)

This table represents the growth in **active internet users** in India from 560 million in the year 2018 to 759 million in 2022, while recording a significant rise in **Aadhaar authentication transactions** to 2,291.97 crore in 2022. In contrast, the number of non-active internet users in the same period has decreased gradually from 540 million to 380 million, reflecting the growing digital reach and impact on biometric services.

Year	Aadhaar Generated (in Crore)	Cumulative Aadhaar Generated (in Crore)	Authentication Transactions (in Crore)	Cumulative Authentication Transactions (in Crore)
2018/19	123.57	123.57	1,080.47	2,896.57

2019/20	125.79	125.79	1,113.54	4,010.11
2020/21	129.04	129.04	1,413.40	5,423.51
2021/22	132.96	132.96	1,771.00	7,194.51
2022/23	136.65	136.65	2,291.97	9,486.48

Table 5: Aadhaar Generation and Authentication Transactions (India) (2018/19 - 2022/23)

This table reflects the growth in Aadhaar generation and authentication transactions from 2018-19 to 2022-23. While the total number of Aadhaar generated has risen from 123.57 crore to 136.65 crore, cumulative authentication transactions have gone up from 2,896.57 crore to 9,486.48 crore, reflecting greater use of this ID for verification purposes across large parts of the country.