# A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORK FOR DATA PROTECTION IN GLOBAL JURISDICTIONS

*Muhammad Zain Alam*
*Chairperson of Cyber & IP Association (CIPA)*
*Law Graduate*
mzainalam66@gmail.com

*Ghaneem Irfan Warraich*
*Managing Director of Cyber & IP Association (CIPA)*
*Law Student*
ghaneem8539@gmail.com

**Abstract**

*Along with the advancement in modern technology, the dependency of people on technology increased. Along with the passage of time, technology became so advanced that crimes entered the realm of cybercrimes. The article highlights the different types of data along with the basic criterion of data protection. This article refers to the critical analysis of global legislations of different states on data protection, how they intend to protect data, how they deal with the crimes such as theft, breach and misuse, and the loopholes in the legislation. All legislations related to data and their methods to tackle the data breach are endorsed, and their loopholes have been highlighted. Though every state has enacted legislation to protect data at its best, a global law is needed to protect data at the macro level. These crimes affect the individuals in the territory of a state but also make the international community vulnerable. There is a need to be proper provisions and clearly stating the jurisdiction and scope of these legislations. The blockchain system is an emerging technology system and can be used effectively to achieve the goal. Data protection is the right of every individual, and it should be preserved.*

**KEYWORDS**: Data, Cybercrimes, Data Protection, Data Breach, Legislation.

## 1. INTRODUCTION

Global legal systems have introduced new trends due to certain types of crimes. The nature of crime is developing with the developed fields of technology in the modern era. Multiple crimes are affecting the states' integrity and violating the rights of individuals. These modern crimes need updated solutions. Global crime statistics show that crimes related to data and personal information are the most affected area. Data is an individual's asset used for welfare at different stages. Multiple

types of data are stored and processed by different databases and servers. Crimes related to data make the person's rights most vulnerable. These crimes include theft, breach, misuse, and other data-related crimes. These crimes affect the individuals in the territory of a state but also make the international community vulnerable. There have been some efforts made by the different legal systems to tackle these crimes within their jurisdiction. Some enacted legislations deal with the aim of data protection in their respective fields. But this area requires some adequate consideration up to the global level, and proper steps should be taken to eradicate this problem. Certain grey areas need special attention both in legislation and practical implementation. Data protection is an aim that has vital importance to eliminate these modern crimes not in domestic but also in international legal systems.

## 2. DATA

Data typically refers to any information, sensitive or confidential, which is stored, processed, or transmitted electronically or in a structured format that can be used as personally identifiable information. It includes facts and figures, concepts, opinions, instructions, and interpretations by humans or automated means.

## 3. TYPES OF DATA

### 3.1 PERSONAL DATA

Personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute, or any other feature of the identity of such a natural person, whether online or offline, or any combination of such features with any additional information, and shall include any inference drawn from such data for profiling (Personal Data Protection Act 2019, § 3(*28*)).

### 3.2 FINANCIAL DATA

Financial data refers to quantitative information collected, processed, and evaluated to measure and analyze an individual's financial status, activities, transactions, and information regarding his financial institutions (Tuovila, 2023). It includes historical and current data such as revenue, expenses, assets, liabilities, cash flow, profits, losses, debt, equity, and other financial ratios and metrics.

### 3.3 TRANSACTIONAL DATA

Transactional data refers to any data generated during a business transaction or financial activity. It includes financial, inventory, and purchasing transactions, the price points of the items bought, the payment method employed, discounts, if any, and other quantities and qualities associated with the transaction (Techopedia).

### 3.4 EMPLOYEES DATA

An employee database is a digital record of information about an individual's employment, job performance, or other work-related activities (Quit Genius, 2021). It may include contact information, job titles, payroll data, social security number, benefits, performance evaluations, and disciplinary actions.

3.5 INTELLECTUAL PROPERTY DATA

Intellectual Property data refers to different types of intangible expressions such as artistic and literary work, discoveries and inventions, words, symbols, and designs (University of Pittsburgh Libraries). Intellectual property data may include details on the ownership, validity, status, and use of these legal rights and information on legal proceedings and litigation involving intellectual property rights.

3.6 HEALTH DATA

Health data means information about the individual's physical or mental health, including his present, past, and future state of health, healthcare services, or healthcare providers. This data may include personal information such as medical history, health conditions, treatment plans, test results, administrative data such as insurance coverage, billing and payment information, and demographic information.

3.7 BIOMETRIC DATA

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics that can be used, singly or in combination with each other or with other identifying data, to establish an individual's identity, such as facial images, fingerprints, iris scans, deoxyribonucleic acid (DNA), face, hand, palm, vein patterns, and voice recordings (GDPR, CCPA/CPRA).

3.8 SOCIAL MEDIA DATA

Social media data refers to social media metrics and demographics collected through analytics tools on social platforms such as Facebook, Twitter, Instagram, and LinkedIn (TechTarget). These data points include blogs, posts, likes, followers, clicks, shares (reposts and retweets), comments, and engagement rates.

3.9 COMMUNICATION DATA

Communication data refers to the information transmitted when individuals communicate using technology, including the electronic messages they send, the social networks they interact with, and the digital documents they create and share (Wright & Shaffer, 2017). It also encompasses metadata, such as the IP addresses of the communication devices, the timestamps of messages, and the geolocations of the devices (Vosoughi et al., 2018).

3.10 GEOLOCATION DATA

Geolocation data is information obtained from electronic devices such as mobile phones, connected cars, smartwatches, Wi-Fi access points, cell towers, or IP addresses. The information is often in the form of coordinate points—longitude and latitude -- which associates a device with a particular physical location (Techopedia).

3.11 WEB-BROWSING DATA

Web-browsing data refers to information collected about an individual's online activity, particularly their use of web browsers to access websites or online services. Browser data includes things such as what websites you visit, where you click, your geolocation, what software and hardware you use, mouse movements, and internet connection information (GCFGlobal, n.d.).

### 3.12 USER-GENERATED DATA

User-generated data refers to content and information data that users generate individually as a result of interacting with the elements that make up any digital market and are shared by users on online platforms or services (J. Park et al., 2021). This can include actions, experiences, feelings, comments, reviews, text, images, videos, comments, reviews, and other forms of content generated by individuals rather than by the platform itself (J. Park et al., 2021).

### 3.13 METADATA

Metadata is the collection of multiple data, which helps to analyze these data more efficiently and descriptively. Metadata is the hub of data which includes web pages, documents, or files, and information about the content of the data, such as keywords, tags, and annotations (TechTarget, n.d.).

## 4. DATA PROTECTION

The concept of Data protection is the process of protecting data which involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy, and the political and legal underpinnings surrounding that data (TechTarget, n.d.). Data protection assures that the data is accessible only for authorized purposes and makes the boundary line for preserving individual privacy. It safeguards crucial information from corruption, compromise or loss, unauthorized access, use, disclosure, modification, or destruction (Kaori, 2019). If the data has been destroyed, it also helps restore it to its functional state and sometimes makes it unusable if necessary.

## 5. IMPORTANCE OF DATA PROTECTION

With the rapid development of artificial intelligence, the amount of data in digital form increased. With the increasing amount of data, various risk factors related to data violation increase (0ECD). Data protection aims to ensure the privacy and security of the information to prevent identity theft, financial fraud, and other types of cybercrime. It involves a range of technical and organizational measures, such as access controls, encryption, firewalls, antivirus software, and data backup procedures.

Data protection is a legal requirement in many jurisdictions around the world. Many legislations endorse data protection as the people's fundamental right, which requires organizations to implement specific data protection measures to help prevent cybercrime and provide individuals with rights related to their personal data (ID4D Guide, 2021).

## 6. DIFFERENT JURISDICTIONS ON DATA PROTECTION

### 6.1 EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR), 2018

GDPR is the first intensive legislation on data protection, which includes multiple rights associated with processing personal data across an extensive range of data contexts. By considering the progressive shifting of the world towards digital data, GDPR introduces the

comprehensive concept of consent for data and bio-sample sharing (European Union, 2016, art. 7). The practical approach is presented by creating legal and social sanctions and considerable penalties for violating GDPR. It further ensures transparency in data sharing and access to the relevant person with consent (European Union, 2016, art. 12).

Through its provisions, GDPR ensures that data shall be processed lawfully and fairly by the data controller with the data subject's consent. Still, it shall be limited to its specific use along with limited data storage. GDPR includes the rights of data subjects related to data access and sharing (European Union, 2016, art. 15, 20). The data subject can consent in written form in understandable, clear, and plain language and have the right to withdraw the consent at any time (European Union, 2016, art. 7). In the case of a child, consent shall be lawful only when the holder of parental responsibility over the child gives it (European Union, 2016, art. 8). At the same time, the bar set by GDPR regarding the minimum age of the child is 13 years which the respective members themselves can set. The data subject has the right to information from the data controller regarding all aspects of his data under process (European Union, 2016, art. 19).

Furthermore, when the processing is done, the data subject has the right to obtain the eradication of all the data available to the controller (European Union, 2016, art. 17). Thus, the controller has an obligation to erase all the data upon request without further delay. GDPR bestows a right to the data subject to file a lawsuit against the organization for the breach of principles of GDPR (European Union, 2016, art. 77). GDPR has provisions to ban a particular organization if it fails to act under its rules and regulations. Also, for every violation of GDPR by organizations, fines of up to 4% of the company's global annual revenue or €20 million, whichever is greater, can be imposed on them (European Union, 2016, art. 83(5)).

### 6.2 US: HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA), 1996

United States introduced its first legislation to protect patients' personal or protected health information (PHI). HIPAA Privacy Rules are the first national standard adopted by the US in data protection (US Department of Health & Human Services, 2023). It regulates PHI's use, access, and disclosure during medical treatment for billing and administrative purposes (HIPAA Privacy Rule: 45 CFR Parts 160 and 164, Subparts A and E). Under HIPAA Privacy Rule, all individually identifiable health information related to healthcare providers, health plans, and clearinghouses is protected (HIPAA Privacy Rule: 45 CFR Parts 160 and 164, Subparts A and E). HIPAA also endorses that the data cannot be shared or accessed unless required by the healthcare provider or with the person's written consent (HIPAA Privacy Rule: 45 CFR § 164.502(a)).

HIPAA Privacy Rule also provides effective penalties of four categories. First, if a person unknowingly violates HIPAA is liable to $100 per violation and a maximum of $25,000 for repeat violations annually (CFR § 160.404(a)(1)). Second, if the breach is backed by reasonable cause, there will be $1,000 per violation and a maximum of $100,000 for repeat violations (CFR § 160.404(a)(2)). Third, if a person willfully neglects HIPAA, he will be entitled to $10,000 per violation and a maximum of $250,000 for repeat violations if the violation is corrected (CFR § 160.406). Fourth, if the offence remains uncorrected, then $50,000 per violation and a maximum

of $1.5 million for repeat violations (CFR § 160.408). If the HIPAA Privacy Rule is violated under false pretences, the penalties can be increased to a $100,000 fine and up to 10 years in prison (CFR § 160.404(b)(2)(iv)).

### 6.3 CALIFORNIA CONSUMERS PRIVACY ACT (CCPA), 2018

The California Consumer Privacy Act is another piece of legislation that plays a vital role in data protection. It opens the door of transparency as it demands the company to show all the information they have about their consumers and list third parties who have access to that data (CCPA, Cal Civ Code §§ 1798.110 & 1798.115). It enhances privacy rights and consumer protection for California residents. CCPA provides the right to know, right to delete, right to opt-out, right to access, and non-discrimination to the resident of California (CCPA, Cal Civ Code §§ §§ 1798.100, 1798.105, 1798.110, 1798. 120, 1798.125). CCPA required the consumers to have the right to know what specific data was collected by the company and also required them to delete that data if needed. They also have the privilege of choosing not to participate in the sale of their personal information. They can access the data held by companies and provide these services to all consumers and residents without any discrimination (CCPA, Cal Civ Code §§ 1798.110 & 1798.125).

If any of these rights are violated, and their data is compromised. In that case, they have the right to file a civil lawsuit or contact the office of the Attorney General for their data preservation (Cal Civ Code § 1798.155(d)) In case of any data breach, CCPA requires these companies to inform their consumers without any delay and take such actions to preserve data and avoid any further violation of data (Cal Civ Code § 1798.82). CCPA allows these businesses and companies to formulate reasonable security measures to protect California residents' data. In case of any violation of CCPA, they will face civil penalties of up to $2,500 per violation or up to $7,500 per violation done intentionally (CCPA, Cal Civ Code § 1798.155(d)). It further provides potential injunction relief to the consumers.

### 6.4 INDIA: THE DIGITAL PERSONAL DATA PROTECTION BILL, 2019

Personal Data Protection Bill is comprehensive proposed legislation in India to ensure privacy rights and data protection provisions. The bill provides several provisions related to data protection, including the right to access, correct, and delete personal data (The Digital Personal Data Protection Bill, § 3, 4, 5, 6). It also restricts or objects to the processing of their personal data. It introduces Personal Data Protection, which includes individuals' privacy relating to the collection, processing, storage, and transfer of personal data by businesses and the government (The Digital Personal Data Protection Bill, § 20). To ensure the transparency of these processes, it includes explicit consent from the individual for any action relating to his personal data (The Digital Personal Data Protection Bill, § 23). It further bound the companies to make a copy of personal data collected from India and other servers in India.

The bill also constitutes the Data Protection Authority of India (DPA) to enforce these rights and provisions. Individuals can file a complaint to the DPA or approach a court of law for the preservation of their data and right to privacy (The Digital Personal Data Protection Bill, § 16). If the data breach occurs, the entity must inform DPA and the affected person immediately. The bill introduces strict provisions for businesses and companies to implement such structure and take

appropriate measures to prevent data breaches and ensure the security of personal data. In case of non-compliance with the provision of the bill, it provides significant penalties, including fines of up to Rs. 15 crores or up to 4% of a business's global turnover or imprisonment for up to three years (The Digital Personal Data Protection Bill, § 82).

### 6.5 BANGLADESH: THE BANGLADESH TELECOMMUNICATION REGULATORY COMMISSION (BTRC), 2002

The BTRC regulation aims to protect individual data and privacy, address cybercrimes, and regulate OTT, digital, and social media platforms. The key feature of BTRC is registering the organization and getting the license as a telecommunication operator, service provider, or equipment manufacturer (The Bangladesh Telecommunication Regulatory Commission, § 11, 12). Yet, there are some conditions to getting the certification. The applicant should be the publisher of online news/ current affairs online content/ publishers of online curated content or web-based programs/films/series. Furthermore, the applicant should have a No Objection Certificate (NOC) from the Ministry of Information to get the license (The Bangladesh Telecommunication Regulatory Commission, § 4). Under this act, an intermediary may be a person, search engines, online sites, cyber cafes, or internet service providers who receive, store, and process an individual's information. An intermediary shall publish the rules and regulations, privacy policy, ad user agreement to the website, which indicates the users regarding the privacy directives. Any information that can instigate the commission of a cognizable offence hurting Bangladesh's integrity, defence, and sovereignty shall also be prohibited while maintaining government secrecy. BTRC restricts sharing any contradictory information creating disharmony in different classes of the community, which would eventually disturb the law and order of the country (The Bangladesh Telecommunication Regulatory Commission, § 27). BTRC pays keen attention to cyberbullying at any level, impersonating another person, harassment of any type for any financial gain, or causing hurt to the other person.

Bangladesh Telecommunication Regulatory Commission is authorized to block any content that puts Bangladesh's sovereignty at stake and disturbs the state's rule of law and international relations. In case of any violation of the act, BTRC may cancel the organization's license or impose a fine on the organization, the amount of which can vary depending upon the severity of the violation (The Bangladesh Telecommunication Regulatory Commission, § 28).

### 6.6 CHINA: PERSONAL INFORMATION PROTECTION LAW (PIPL), 2021

China formulated data protection provisions by enacting Personal Information Protection Law in 2021. Like other legislations, they also introduce individual consent for collecting, using, or processing their personal information (PIPL 2021 § 13, 15). The act further provides individuals with the right to access, correct, and delete their personal information, as well as the right to request that businesses stop using or processing their personal information (PIPL 2021 § 16). They also regularize the data collection in the territory of China and formulate the office of the Data Protection Officer to regulate the act's provisions (PIPL 2021 § 38). The law imposes strict provisions related to sharing data outside China's territory, including explicit consent of the individual and conducting security assessment (PIPL 2021 § 39).

In non-compliance with the act, the complaint can be filed to the relevant regulatory

authority, such as the Cyberspace Administration of China or the National Information Security Administration. Businesses must notify the individual and relevant authorities if there is a data breach. This non-compliance and breach also dealt with penalties and fines of up to RMB 50 million (approximately USD 7.7 million) or 5% of the business's annual revenue and potential suspension of business operations or revocation of business licenses (PIPL 2021 § 66). Additionally, companies may be liable for any damages caused by violating the PIPL.

### 6.7 CANADA: THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA), 2000

The personal information protection and electronic documents act sets out rules and regulations for organizations regarding the personal information of individuals. The act provides comprehensive consent of the data holder, who fully understands the conditions for collecting, using, and disclosing his personal data (The Personal Information Protection and Electronic Documents Act, § 6). An organization may collect information without the individual's consent if the consent cannot be obtained in time or it deems fit in the person's interest. In case of an emergency and to protect life, PIPEDA allows an organization to use an individual's personal information for investigation without his consent (The Personal Information Protection and Electronic Documents Act, § 7). The act provides an exception that an individual's personal information can be disclosed without his knowledge or consent when he owns a debt to an organization or is declared a threat to the sovereignty of Canada.

PIPEDA gives the authority to the privacy commissioner to deal with the reports made by the organizations in case of any threat or breach of security to an individual's personal data. The commissioner issues his report after his findings and recommendations to both parties and shall send the report to both parties within one year (The Personal Information Protection and Electronic Documents Act, § 11, 12). Not being satisfied with his decision, the complainant may appear before the court, which, along with damages and other remedies to the complainant, may order the organization to mend its work style. In case of any negligence of PIPEDA, a fine of up to $100,000 may be imposed on the organization (The Personal Information Protection and Electronic Documents Act, § 16).

### 6.8 AUSTRALIA: THE PRIVACY ACT, 1988

The Privacy Act 1988 is another step towards data protection through proper legislation in Australia. It applies to most private and public sector organizations and sets specific requirements for using, collecting, and processing data (The Privacy Act 1988, § 14, 15). The major change is set by introducing 13 Australian Privacy Principles regarding obtaining consent, providing individuals access to their personal information, and notifying individuals of data breaches. It also includes the concept of consent for data processing. It introduces the rights to access and corrects their personal information and the right to complain if they believe their privacy rights have been breached (The Privacy Act 1988, § 16A). The act also introduces privacy policies that set out for the business to handle the personal data of individuals.

To file a complaint related to privacy under the Privacy Act 1988, individuals can complain to the Office of the Australian Information Commissioner (OAIC) (The Privacy Act 1988, § 23). The OAIC can investigate complaints and take enforcement action against businesses that breach

the APPs. The remedies available in case of a breach of privacy under the Privacy Act 1988 include compensation for any loss or damage suffered due to the breach (The Privacy Act 1988, § 41). In addition, penalties and fines can be imposed on businesses that breach the APPs (The Privacy Act 1988, § 47). The maximum penalty for serious or repeated privacy breaches under the Privacy Act 1988 is $2.1 million for businesses and $420,000 for individuals (The Privacy Act 1988, § 13G(1)).

### 6.9 SOUTH AFRICA: THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA), 2021

The Protection of Personal Information Act is a South African law binding on private and public bodies of the country. It is enacted to give effect to the constitutional right to privacy and the protection of individuals' private data. Its main purpose is to create a safe and healthy environment in which organizations can store and process an individual's personal data without any threat to the data. To collect personal data, it is the duty of the data collector to make the data subject familiar with the name and address of the responsible party, the reason why the data is being collected, and the consequence of the failure to provide information (The Protection of Personal Information Act, § 5). At the same time, an organization can only access, process, or store the data only after obtaining the consent of the individual while having the right to withdraw the consent at any time (The Protection of Personal Information Act, § 11, 12). A competent person can consent in the case of a child according to the country's law (The Protection of Personal Information Act, § 34). Meanwhile, the organizations must not keep the data record longer than authorized by the law to keep in possession or longer than the period fixed by the parties in the contract.

There have been certain exceptions in POPIA that it doesn't apply to the information that has been de-identified in any form and cannot be used again to identify the person, the information which can be a threat to the national security of South Africa or the information that can be helpful in any legal proceeding (The Protection of Personal Information Act, § 15). Individuals aggrieved by the breach of POPIA can claim remedies. POPIA can award imprisonment for a maximum period of 10 years with or without a fine, while the administrative fine is up to R10 million for non-compliance to the act's provisions (The Protection of Personal Information Act, § 107, 109).

## 7. LEGISLATION ON DATA PROTECTION IN PAKISTAN

### 7.1 PREVENTION OF ELECTRONIC CRIMES ACT, 2016

The Prevention of Electronic Crimes Act (PECA) was adopted to provide security to the data of common masses and prevent cybercrimes. PECA highlights the cybercrimes such as hacking, cyberstalking, cyberbullying, spreading false information, etc. and provides punishments for the offenders. However, PECA was thought to violate the fundamental right of freedom of speech and expression, i.e., Article 19 of the Constitution of the Islamic Republic of Pakistan (Azam, 2021). Still, the government declared it essential to prevent cybercrime and to flourish the actions taken to protect data. PECA provides data privacy rights, including data collection, processing, and use (Prevention of Electronic Crimes Act, §31). The personal information of a person shall be held by the data controller, who will be bound to give access and make any change at the request of the particular individual (Prevention of Electronic Crimes Act, §34). PECA

requires the data controller to notify the individual immediately in case of any data breach (Prevention of Electronic Crimes Act, §31(3)).

PECA bestows the right to file a complaint to relevant authorities if an individual doubts that his right to data protection has been infringed at any level (Prevention of Electronic Crimes Act, §37). The complaint shall be made to the Cyber Crime Wing of the Federal Investigation Agency (FIA), which must contain the details of the data breach (Prevention of Electronic Crimes Act, §37(2)). After a thorough investigation, FIA Cyber Crime Wing shall fine the offender up to PKR 50 million (approx. USD 32000) depending upon the nature of the violation (Prevention of Electronic Crimes Act, §37(4)). Also, victims can approach an appropriate court to seek remedies for the breach of their personal data (Prevention of Electronic Crimes Act, §38). Under PECA, a person could be fined up to PKR 5 million (approximately USD 31,500) and imprisonment for up to 2 years, or both for unauthorized access or transmission of data, up to PKR 1 million (approximately USD 6,300) and imprisonment for up to 3 years, or both for cyberstalking, up to PKR 50 million (approximately USD 315,000) and imprisonment for up to 14 years, or both for cyberterrorism, and up to PKR 50 million (approximately USD 315,000) and imprisonment for up to 7 years, or both for malicious code (Prevention of Electronic Crimes Act, §3, 6, 10, 24).

### 7.2 PERSONAL DATA PROTECTION BILL 2021

After PECA, the government of Pakistan took another step to ensure data protection at every level and introduced Personal Data Protection Bill 2021. It is still in the process to be enacted, but it is hoped that when it is enacted, it will create a safe atmosphere for the flourishment of personal data. It provides a legal framework for organizations and governments to follow certain protocols while dealing with the data. This government has tried its level best in this bill to ensure lawfulness, transparency, and fairness regarding the data protection of individuals. This bill highlights the necessity of the data subject's consent for collecting, processing, storing, and transferring personal data (Personal Data Protection Bill, § 4, 5, 6, 7, 8 ). The bill provides the data subject with the right to access, correct, and notify in case of a data breach, which is the bill's key feature (Personal Data Protection Bill, § 13 ). Furthermore, the punishments are also defined, and fines have been fixed for non-observance of the bill. For the purpose of this bill, the federal government shall constitute the National Commission for Personal Data Protection (NCPDP) which will have the same powers as vested by a civil court with the virtue of Code of Civil Procedure Code, 1908 (Personal Data Protection Bill, § 32, 33, 34).

This bill provides certain penalties for not being able to cope with the provisions of the bill, which can be changed a bit before its enactment. In case of failure to abide by the rules and regulations regarding data protection, a company can be fined up to PKR 25 million or 4% of the company's annual turnover, whichever is higher (Personal Data Protection Bill, § 34(1)). Whereas for processing of the data without consent and failure to notify the individual about the data breach, a fine of up to PKR 5 million or 2% of the company's global turnover, whichever is higher, can be imposed on the company (Personal Data Protection Bill, § 35(1)). And for unauthorized transfer of personal data and violation of the individual's data protection rights, a fine of up to PKR 10 million or 2% of the company's global turnover, whichever is higher, may be imposed on the company(Personal Data Protection Bill, § 36(1)).

## 8. COMPARATIVE ANALYSIS

Data protection is critical in today's fast-shifting world of electronics and technology. In this technology-dominant era, all the personal data of people is available everywhere. These new trends make the data of individuals vulnerable, and data theft has become easy for criminals. Different states and international organizations try to tackle the issue by proposing certain legislation (Arab, 2020). Due to this surge, every country around the globe has enacted legislation to prevent cybercrimes and data theft and ensure data protection, some of which are discussed above. These key legislation provide individual consent for using, processing, collecting, and transferring data (Pearson, 2009). These laws make it explicit to have consent for performing any data-related action. It also requires written authorization for the use and disclosure of health information. Despite massive advancements in technology, the issue lies that many people are still unaware of cybercrimes and threats to their data. These laws constitute the right to data privacy as a basic fundamental right of human beings (Pearson, 2009). Many people are unfamiliar with data theft and cybercrimes and how to prevent them.

These legislations also provide multiple rights to individuals, including the right to access, delete, construct, share, abstain, and remove. These rights produce certain obligations on the companies and businesses towards their consumers and residents. An individual can have all the necessary information regarding any data usage. What makes these rights vulnerable is the lack of a defined mechanism for their implementation. Many legislations are lacking behind because of non-generality in the implementation of these rights (Berggren, 2000). As stated above, multiple laws only apply to a specific group of companies. The next hurdle is the scope of these rights are not introduced in all sphere of data protection. Some laws deal with healthcare information, others with commercial information, but very few deal with electronic or social media data (Büschel et al., 2014). Multiple platforms use individuals' personal data without being notified to them. In that case, these rights are another overflowing piece of legislation without implementation.

To tackle these legislations with a uniform process, they also establish a Data Protection Authority to oversee and enforce data protection regulations. These authorities have multiple jurisdictions that are ineffective enough to console the individual regarding his data violation (Ajayi, 2016). They introduce the penalties: fines, restraining orders, and imprisonment. These punishments are not in good faith with the victim of these crimes. The fine goes to the government, and the person behind bars will suffer his punishment, but the victim is not provided with the proper remedy. No provisions state the recovery of data and compensation to the person whose data is violated.

Indeed, these legislations play a vital role in preventing crimes related to data and personal information. Certain loopholes still open the door to data breaches and unlawful use of personal information. These legislations need new provisions to ensure data safety and protection, mainly data recovery at all costs (Pearson & Benameur, 2010). There is a need to do more work on the proper mechanism and comprehensively providing data protection to users.

## 9. POLICY RECOMMENDATION

Based on the legislations mentioned above and the facts, data protection still needs special

attention and serious actions. The grey area is the data breach and data theft in this matter. To tackle these, we must spread awareness regarding cybersecurity, cyber protection, cybercrimes, and data protection. This awareness can be done by adopting multiple effecting policies by organizations and governments. There needs to be an international platform that promotes generality and transparency in data protection, usage, access, sharing, and processing.

Regarding consent and notifying, the procedure needs to be amended according to human psychology. As many websites and platforms modify by popping up the cookies button, it should be replaced by a thirty-second animated video that effectively tells people about a part of their data will be shared. In this way, we can apply the concept of consent in its true essence.

The main concern of all individuals is data protection and data recovery. Besides producing comprehensive legislation, we must adopt a practical approach to this issue. A blockchain can be introduced to protect multiple folds of data, and in case a data breach occurs, it can save a significant part of the data. This blockchain program can also allow us to recover any lost data with a specific security checkup. By adopting these, we can achieve the goal of data protection in this technology-oriented era.

## 10. CONCLUSION

Indeed data protection is vitally important for the elimination of these modern crimes. Multiple crimes deal with data such as cyber theft, cybercrimes, data breach, and misuse of data, transactional records, and other important information which can impact an individual's life. These crimes are enhancing day after day, and their impacts are on a global level. These crimes need to be addressed, and these should be tackled. The three ways to tackle these crimes are; proper effective legislation, implementation of the procedure, and practical and scientific approach to handling these crimes. As mentioned above, specific legislations are not comprehensive, and some have limited scope. There is a need to be proper provisions and clearly stating the jurisdiction and scope of these legislations. All these efforts are useless if they cannot be implemented in the legal systems of each state. The data breach is not a national issue but pertains to an international issue. So it also must be addressed on international platforms, and proper steps should be taken from these platforms. The blockchain system is an emerging technology system and can be used effectively to achieve the goal. Through these steps, the goal of data protection can be fulfilled. As modern problems require a modern solution, this is the key to solving crimes related to data. Data protection is essential to our systems, and proper attention is needed for this section. Data protection is the right of every individual, and it should be preserved.

## Bibliography

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1-12.

Arab, M. S. (2020). Global surge in cybercrimes-Indian response and empirical evidence on need for a robust crime prevention system. International Journal of Cyber Criminology, 14(2), 497.

Azam, M. (2021). Pakistan's international law obligations and curtailment of freedom of expression: Balancing legitimate competing interests or a case of violation? Pakistan Law Review, 12.

Berggren, N. (2000). Implementing generality while reducing the risk for fiscal explosion. Constitutional Political Economy, 11(4), 353-369.

Büschel, I., et al. (2014). Protecting human health and security in digital Europe: How to deal with the "privacy paradox"? Science and Engineering Ethics, 20, 639-658.

California Consumer Privacy Act (CCPA) (2018).

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2023] OJ L119/1, art. 7.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2023] OJ L119/1, art. 12.

GCFGlobal. (n.d.). Understanding browser tracking. GCFGlobal. Available at: https://edu.gcfglobal.org/en/internetsafety/understanding-browser-tracking/1/ [Accessed 26 March 2023].

HIPAA Privacy Rule (1996).

Ishii, K. (2019). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: Looking at functional and technological aspects. AI & Society, 34, 509.

J. Park, et al. (2021). The effect of user-generated data on hotel booking: A moderated mediation model. Tourism Management, 40, 104257.

Kaori, I. (2019). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: Looking at functional and technological aspects. AI & Society, 34, 509.

OECD. (n.d.). OECD iLibrary. Available at: https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en# [Accessed 7 April 2023].

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. In 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing (pp. 44-52). IEEE.

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In 2010 IEEE Second International Conference on Cloud Computing

Technology and Science (pp. 693-702). IEEE.
Personal Data Protection Act 2019 (India).
Personal Data Protection Bill 2021 (India).
Personal Information Protection and Electronic Documents Act (PIPEDA) (2000).
Personal Information Protection Law (PIPL) (2021) (China).
Prevention of Electronic Crimes Act (PECA) (2016) (Pakistan).
Techopedia. (n.d.). Data protection. Available at: https://www.techopedia.com/definition/29406/data-protection [Accessed 28 March 2023].
Techopedia. (n.d.). Geolocation data. Available at: https://www.techopedia.com/definition/30654/geolocation-data [Accessed 26 March 2023].
Techopedia. (n.d.). Transactional data. Available at: https://www.techopedia.com/definition/30367/transactional-data [Accessed 25 March 2023].
TechTarget. (n.d.). Metadata. Available at: https://www.techtarget.com/whatis/definition/metadata [Accessed 26 March 2023].
TechTarget. (n.d.). Social media analytics. Available at: https://www.techtarget.com/searchbusinessanalytics/definition/social-media-analytics [Accessed 26 March 2023].
Thales Group. (n.d.). Biometric data and privacy laws (GDPR, CCPA/CPRA). Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data-and-privacy-laws-gdpr-ccpacpra [Accessed 25 March 2023].
The Bangladesh Telecommunication Regulatory Commission.
The Digital Personal Data Protection Bill, 2019 (India).
The Privacy Act 1988 (Australia).
The Protection of Personal Information Act 2013 (South Africa).
Tuovila, A. (2023, January 21). Financial analysis: Definition, importance, types, and examples. Investopedia. Available at: https://www.investopedia.com/financial-analysis-4689863 [Accessed 25 March 2023].
University of Pittsburgh Libraries. (n.d.). Copyright definitions. Available at: https://pitt.libguides.com/copyright/definitions [Accessed 26 March 2023].
US Department of Health & Human Services. (n.d.). Laws & regulations. Available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html [Accessed 7 April 2023].
Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146.
World Bank. (2021). Data protection and privacy laws. ID4D Guide. Available at: https://id4d.worldbank.org/guide/data-protection-and-privacy-laws [Accessed 7 April 2023].
Wright, D., & Shaffer, J. (2017). Advancing research on digital communication: A framework for

capturing and analyzing electronic interaction data. Communication Methods and Measures, 11(4), 263.