VOLUME 4 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

COMPARATIVE ANALYSIS OF DPDP ACT 2023 AND GDPR CONCERNING CROSS-BORDER TRANSFER OF DATA, RIGHT TO PRIVACY, AND DATA BREACHDURING THE COVID-19 PANDEMIC

- Umang Raitani[1] & Anuj Deshmukh[2]

Abstract

This scholarly examination compares the European Union's General Data Protection Regulation and India's Digital Personal Data Protection Act 2023. The research is structured around three pivotal aspects of data privacy laws: cross-border data transfer, data breaches during the COVID-19 pandemic, and the interpretation of Right to Privacy. The study scrutinizes the legal provisions regulating cross-border data transfer under GDPR and the DPDP Act 2023. It aims to discern the effectiveness of these regulations in safeguarding data during transactional exchange, a critical concern in our increasingly globalized digital space. The research further investigates the surge in data breaches during the COVID-19 pandemic. It examines the notable instances of the breaches, evaluates the response mechanisms, and assesses the efficiency in mitigating such violations. The right to privacy is the cornerstone of both the regulations. The research explores its legal interpretation and enforcement under GDPR and DPDP Act 2023, offering a comparative analysis that underscores their implications for individual privacy rights.

Keywords: - (COVID-19, Cross Border data transfer, Data Breach, Data transfer, Digital Personal Data Protection Act 2023(DPDP Act), General Data Protection Regulation (GDPR), Right to privacy)

Introduction

[1]Umang Raitani, LLM Student Symbiosis Law School, Pune
[2]Anuj Deshmukh, LLM Student Symbiosis Law School. Pune

Data privacy has become one of the most important subjectsfor the government and businesses in the digital age.Therefore, it has made individuals concerned about their data, its protection, and their privacy concerning the handling of data by organizations. Data protection is becoming a critical issue in today's world. With the increasing quantityof data being collected and processed, it is more important to ensure that the data is protected from unauthorized access, use, or disclosure and from being stolen. Two of the most comprehensive data protection laws in the globalizing world are The GDPR of the European Union and The Digital Personal Data Protection Act 2023 of India, passed on 4 August 2023. Both laws impose strict requirements on the organizations that collect, process, or transfer personal data. One of the critical areas where the GDPR and the DPDP Act differ is their way of dealing with cross-border data transfer. The GDPR requires organizations to obtain explicit and explicit consent from the data subjects before transferring their data to a foreign country. The DPDP Act, on the other hand, takes a more relaxed approach. It allows the organizations to transfer data to any country without obtaining the express consent of the users unless the central government has notified that country as the country to which data transfer is strictly prohibited. Article 12 of the constitution of India guarantees the right to privacy to all citizens. In the landmark case of K.S Puttaswamy V Union of India, the Supreme Court held that privacy is a fundamental right protected under Article 21 of the Constitution of India. The Court also held that the right to privacy includes the right to control one's personal information. Data is the new gold of the 21st century, and it is essential to be protected from unethical hackers, cyber terrorists, or any other unwanted entity that intends to misuse the data for dishonesty. Data transfer and transmission are always under constant threat due to the ever-dynamic and evolving digital world, for it is where this gold of the 21st century exists. Hence, a robust system of deterrence that deals with data transfer across bordersand regulations that guard the privacy of the data principles is required. The European Union's regulations, which are the basic globally recognized rules, and India's newly enacted legislation on the data protection act as the necessary deterrence. The Indian laws and regulations have been recently developed on the sidelines of the data breaches during the pandemic. Thus, the legislation Digital Personal Data Protection Act 2023, after many revisions, came into existence.The very concept of data protection means measures and practices to be adopted and implemented to secure the rights of individuals relating to their digital existence. Personal data is any information that can be used to identify and recognize

an individual or individuals, such as name, address, mobile numbers, email ID, and even health-related data, amongst many more. The need for data protection is the call of the hour due to the ever-increasing reliance on digital equipment. Data protection laws vary across jurisdictions and nations. The legislation for data protection should have a robust mechanism in place to deal with any possible mishap to an individual's data. It is of the utmost importance to maintain the confidence between the data principles and the data fiduciaries through a transparent method of compliance for both the data principles and data fiduciaries.

Relevance of Topic in Contemporary Scenario

Data protection is increasingly relevant in the contemporary scenario, given the growing volume of data being dealt with by governments and corporations. The cross-border transfer of personal data is highlyapplicable as businesses and organizations operate in multiple jurisdictions. The COVID-19 pandemic has further highlighted the importance of data protection, as there have been several high-profile cases of data breaches involving the personal data of millions of individuals. These data breaches have raised serious concerns about the security of the personal data. The comparative analysis of the GDPR and The DPDP act concerning cross-border transfer of data is relevant in the contemporary scenario as it can help to identify the best practices, shed light on the opportunities and challenges associated with cross-border data transfers, and also because it can help promote harmonization of data protection laws and policies across various regions around the globe. The recent cases of data breaches in India during COVID-19 highlight the need for stricter data protection enforcement mechanisms. The DPDP Act is expected to address these concerns. The rise of AI and ML (machine learning) technologies is leading to the collection of personal data, which also raises significant privacy concerns. IoT devices such as smartphones and smartwatches collect data about our daily activities. This data can be used to monitor our health, track our activities, and target us with advertising.

Statement of Problem

In the era of digitalization, data protection and privacy have become paramount. The GeneralData Protection Regulation and The Digital Personal Data Protection Act 2023 have been implemented to safeguard the individual’s data rights. However, the effectiveness of these regulations in cross-border data transfer and during the COVID-19 pandemic has seen

an unprecedented surge in data breaches and remains a significant concern. Furthermore, the interpretation and implementation of the right to privacy under both these regulations need a thorough investigation.This research aims to compare the GDPR and the DPDP Act 2023 to understand their effectiveness in data privacy, their response to data breaches, and how they uphold the right to privacy.

Research Questions

1. How do the DPDP Act and GDPR differ in regulating cross-border data transfer?
2. How does the DPDP Act strengthen the right to privacy under Article 21 in India?
3. What are the recent cases of data breaches in India during Covid 19?

Research Objectives

1. To compare and contrast the DPDP Act and GDPR concerning their regulation of cross-border data transfers.
2. To document recent cases of data breaches in India during Covid 19.
3. To assess how the DPDP Act strengthens the right to privacy in India.

Research Methodology

1. Qualitative Method – This method includes understanding the reason behind the intent of the legislative to frame such a concept and to analyzeits perspective.
2. Observatory Method –This method employs a secondary research type of methodology, such as literature evaluations, which include reviews of textbooks, Wikipedia, journal articles, and newspaper articles.

Scope And Limitation

The scope of this research encompasses a detailed comparative analysis between The General Data Protection Regulation and the Digital Personal Data Protection Act 2023. The research focuses on three main areas: cross-border data transfer, data breaches during the COVID-19 pandemic, and the right to privacy. It aims to provide valuable insights for stakeholders, including policymakers, businesses, and individuals, to understand better and navigate the complex data protection and privacy area. However, this research has limitations. One significant limitation is the availability of cases related to data breaches during the pandemic. Not all breaches are made public or reported, which could limit the comprehensivenessof the

research in this area. Furthermore, the research is limited by the evolving data protection measures as new rules and regulations are constantly being enacted. The research also does not cover the other aspects of the GDPR and The DPDP Act due to the vastness of these regulations.

Literature Review

1. **Critical Analysis: Digital Personal Data Protection Bill 2022[3]: -**In India, the Digital Personal Data Protection Bill 2022 attempts to deal with the issue of data privacy and protection of digital rights in the digital world. Thecriticalgoal is to set the standards for the processing of digital personal data that upholdpeople's right to privacy, ensure the necessity and legality of data processing, and prevent personal data breaches and thefts. Fairness, openness, purpose, limitation, data minimization, accuracy, storage, limitation, and accountability are some parameters and criteria outlined in the bill for data fiduciaries.Also, the new legislation includes new clauses and provisions from the earlier versions of the act. It includes, for example, the right to post-mortem privacy, which allows a designated person to exercise the rights of a data principal in the event of incapacity or death. It permits cross-border data transfer under specific conditions, resolving significantissues concerning the tech giants. The new provisions also levy harsh penalties for noncompliance with the rules by data fiduciaries, with the number of penalty amounts increasing to a greater extent than the earlier legislations.However, many objections and worries are troubling the measure tech companies and the organizations engaged in handling data. One crucialproblem is the lack of a legislative framework to protect sensitive personal data since the law makes no distinction between different forms of personal data. In other words,the idea of "deemed consent" has also raised a lot of concerns about the possible exploitation of personal data. The new legislation repeals the prior clause requiring data localization, which may have unforeseen circumstances for data sovereignty and security of the data principles. There are also doubts concerning the Data Protection Board's composition and authority and the lack of time for many tasks that will be dealt with under it.

[3]Aditya Bashambu& Lavanya Chetwani, Critical Analysis: Digital Personal Data Protection Bill 2022, 3 Jus Corpus L.J. 519 (2022).https://www.juscorpus.com/wp-content/uploads/2023/01/108.-Adiyta-Bashambu-and-Lavanya-Chetwani.pdf

2. **The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards[4]: -** The above paper presents a complete and in-depth examination of the DPDP Act and GDPR, emphasizing cross-border data transmission and the right to privacy.The paper summarizes the DPDP Act and GDPR, highlighting the essential similarities and distinctions. The writer has discussed the DPDP Act and GDPR requirements relating to cross-border data transmission and the right to privacy.Regarding cross-border data transfers, the author observes that, unlike the GDPR, the DPDP Act does not provide a blanket restriction on such transfers. Instead, the DPDP Act permits cross-border data transfers to nations identified as "approved" by the Central Government. The analysis of the DPDP Act's additional options for cross-border data transfers, such as permission and standard contractual terms, has also been mentioned.Regarding privacy, it is pointed out that the DPDP Act allows data principles greater control over their data than the GDPR. For example, under the DPDP Act, data principals have the right to erase their data, which is not clearly stated in the GDPR. Finally, it is said and accepted that the DPDP Act is a big step forward for data protection in India. However, there is an opinion that the DPDP Act might be improved in several respects, such as by establishing more specific enforcement provisions.The author addresses the DPDP Act's and GDPR's respective approaches to cross-border data transmission. The DPDP Act authorizes the Central Government to designate nations as "approved" for cross-border data transfers. The GDPR prohibits any cross-border data transfers to countries outside the European Economic Area (EEA) unless the nation is assessed to have an "adequate" level of privacy protection.
3. **The Digital Personal Data Protection Bill 2022 in Contrast with the EU General Data Protection Regulation: A Comparative Analysis[5]: -**The above literature discusses the specific sections of the DPDP Act and GDPR relating to the right to privacy.According to the writer, the DPDP Act and the GDPR recognize privacy as a fundamental right. However, the article points out some significant defects in how the two statutes guarantee the right to privacy. The GDPR, for example, provides a broader definition of personal data than the

[4]Kuner, Christopher, The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards (November 20, 2021). National Law Review of India, vol. 33 no. 1 (2021), Available at SSRN: https://ssrn.com/abstract=3964672

[5]Adv. Ashwini Kumar, The Digital Personal Data Protection Bill 2022 in Contrast with the EU General Data Protection Regulation: A Comparative Analysis, 5 IJFMR 3 (2023).https://www.ijfmr.com/papers/2023/2/2534.pdf

DPDP Act. The GDPR defines personal data more broadly than the DPDP Act. The GDPR also offers data subjects more control over their data, such as the right to delete the data. There are many enforcement tools available under the DPDP Act and GDPR. The GDPR has more robust and more complying enforcement methods than the DPDP Act. The DPDP Act is a big step forward for India's privacy rights. It also argued that the DPDP Actwould be improved in manyaspects, such as by establishing more to-the-point and apt enforcement procedures and through interpretations by the judiciary over time.

4. **Cross-border Transfer of Personal Data under the Digital Personal Data Protection Bill 2022: A Comparative Analysis[6]: -**The DPDP Act and GDPR are the world's most comprehensive data protection regulations. Their approaches to controlling cross-border data flows differ. The GDPR restricts data transfers to countries outside the EEA unless they are assessed to have an "adequate" level of data protection. Still, the DPDP Act permits cross-border transfers to countries designated "approved" by the Central Government. The DPDP Act also includes a variety of alternative cross-border data transmission procedures, such as permission, standard contractual agreements, and derogations.These methodological disparities have repercussions for enterprises and organizations that operate in several jurisdictions. Businesses subject to the GDPR must take extra precautions to verify that their cross-border data transfers are legal. Businesses subject to the DPDP Act will have greater freedom regarding cross-border data transfers but must still comply with the Act's provisions.These methodological disparities have repercussions for enterprises and organizations that operate in several jurisdictions. Businesses subject to the GDPR must take extra precautions to verify that their cross-border data transfers are legal. Businesses subject to the DPDP Act will have greater freedom regarding cross-border data transfers but must still comply with the Act's provisions.It's worth noting that the DPDP Act is still in its early implementation phases. It remains to be seen how the Indian government will interpret and execute the Act.The article does not address the difficulties associated with implementing the DPDP Act and GDPR in the context of cross-border data transfers. Also, the article does not mention data privacy regulators' involvement in encouraging cross-border data flows.Also, it

[6] Cross-Border Transfer of Personal Data under the Digital Personal Data Protection Bill 2022: A Comparative Analysis, TSAARO (Jan. 5, 2023), https://tsaaro.com/blogs/cross-border-data-transfers-under-the-digital-personal-data-protection-bill-2022/

does not mention the future of cross-border data transfers in light of the DPDP Act or the GDPR.

5. **India's Data Protection Framework Will Need to Treat Privacy as a Social and Not Just an Individual Good[7]: -**The consent model in the data protection legislation is restricted under data protection regulations by depending on individuals to make informed decisions regarding the handling and using personal data. However, privacy warnings are often extensive, making it difficult for users to understand and make meaningful decisions. Furthermore, with the continuous collection of data by and fromdigital services and methods, it is almostimpossible for individuals to expressvalid and efficient consent. The amount of data being gatheredcontinuously increases, and individuals have no idea how their data will be collected, bifurcated, and used. This compromises the consent model's efficacy in preserving individuals' data control.In legislation, looking at privacy as a social good is crucial because it recognizes that privacy is not only an individual right but also a desired and collective aim for society. Personal growth and preserving social interactions that rely on selective self-presentation require privacy. Instead of depending exclusively upon market forces, authorities should prioritize maintaining and promoting privacy by defining it as a social benefit. This point of view accepts that protecting individuals against others' negligent management of their data involves social cooperation and collective action. To defend privacy as a social good, policymaking should not be value-neutral but adopt normative views on data collecting, processing, and sharing practices.

How do the DPDP Act, 2023, and GDPR differ in regulating cross-border data transfer?

Introduction: -

Two crucial data protection laws that aim to secure people's personal information and encourage responsible data handling are the General Data Protection Regulation (GDPR) of the European Union and the Digital Personal Data Protection Act 2023 (DPDP Act) of India. Even if their objectives are similar, they differ significantly regarding implementation, scope, and particular clauses. Their objectives include safeguarding people's privacy, granting rights to data subjects, and putting in place solid systems for compliance and data protection.

[7]Sinha, Amber. "India's Data Protection Framework Will Need to Treat Privacy as a Social and Not Just an Individual Good." Economic and Political Weekly, vol. 53, no. 18, May 5, 2018, pp. 18-21.

Despite their many parallels, some provisions, like the necessity of data localization, the appointment threshold for data protection officers, and the severity of fines, differ. Comprehending these disparities is of utmost importance for establishments functioning within the regulatory structures of India and the EU, guaranteeing adherence to the particular demands of every regulation. Here are some of the similarities

- Data Subject Rights: The GDPR and the DPDP Act 2023 both emphasize how important it is to give people a robust set of rights regarding their data. These rights include the ability to see what personal information is kept on them by organizations, correct errors, and ask for their data to be deleted in certain situations. Furthermore, both statutes allow individuals to withdraw their consent for data processing to provide data subjects more control over their personal information.
- Consent Requirements:Before processing a person's data, both regulations require organizations to have that person's explicit and informed consent. People will be fully informed about how their data will be used and will have the chance to make educated decisions thanks to this shared emphasis on explicit and affirmative consent.
- Data Breach Notification: Provisions for data breach notifications are introduced by the GDPR and the DPDP Act 2023. They require companies to immediately notify the appropriate authorities and impacted parties of data breaches. This criterion facilitates quick responses to data security issues while improving accountability and openness.
- Data Protection Officers (DPOs): The significance of supervising data protection compliance within organizations is acknowledged by both statutes. They mandate the appointment of Data Protection Officers (DPOs) by specific entities, whose job is to ensure that data protection regulations are followed. DPOs are essential in helping to ensure compliance and acting as contacts for issues about data protection.
- Special Categories of Data: The GDPR and the DPDP Act 2023 both provide stronger protections for some types of personal data, including biometric and health data. Sensitive data processing necessitates specific consent and more robust guidelines, recognizing the need for improved privacy protections for this kind of data.
- Accountability and Documentation: The significance of accountability and documentation is stressed in both rules. They mandate that businesses keep documentation of all data

processing operations and prove they adhere to data protection regulations. Increased regulatory monitoring and openness are two benefits of these actions.

- Penalties and Fines: Failure to comply with data protection requirements may result in penalties and fines under the GDPR and the DPDP Act 2023. Although the two legislations may differ regarding the severity and format of these sanctions, both share the idea of making companies responsible for data protection breaches.

They share core principles but also differ w.r.t scope, regulatory approach, and specific provisions. The critical distinctions between these two data protection regulations:

1. Geographical Scope and Liability: DPDP Act 2023, unique to India, applies to organizations that handle personal data there. Its extraterritorial applicability extends to non-Indian organizations that handle the data of Indian citizens.

The General Data Protection Regulation (GDPR) applies to entities that handle personal data of individuals within the European Union (EU) and extends its jurisdiction to entities outside the EU that hold data of EU citizens. Its impact is more widespread internationally.

2. Data Localization Requirements: The DPDP Act 2023 requires sensitive personal data to be localized and a copy of that data to be kept within the borders of India. This is to guarantee that some types of data stay under national control.

GDPR localizing data is not necessary under GDPR. Its main goal is to control cross-border data transfers and guarantee that sufficient security measures are implemented when transferring data outside the European Union.

3. Data Breach Notification Timelines: DPDP Act 2023 establishes deadlines for notifying the Data Protection Authority and impacted parties of data breaches. These deadlines might not match the GDPR's specifications.

GDPR: GDPR establishes a very quick notification obligation by enforcing a rigorous 72-hour timeframe for notifying affected parties and supervisory authorities of data breaches.

4. Data Protection Officers (DPOs): DPDP Act 2023: Depending on the precise requirements stated in the regulation, the DPDP Act may or may not mandate the appointment of Data Protection Officers (DPOs). GDPR: GDPR expands the need for DPOs by requiring their appointment for some organizations, especially those handling sensitive or large-scale data.

5. Penalties and Fines: The DPDP Act establishes a system of fines and sanctions that may vary from the GDPR regarding severity and thresholds. Depending on the seriousness of the infraction, penalties may consist of fines and sanctions.

GDPR: Depending on the severity of the infraction, non-compliance with GDPR can result in fines of up to 4% of a company's yearly worldwide turnover or €20 million, whichever is larger. It is generally acknowledged that the sanctions under GDPR may be rather severe.

6. Data Subject Representative and European Data Protection Representative: DPDP Act 2023: This legislation may contain provisions about the designation of a Data Subject Representative for non-Indian organizations that handle the personal data of Indian citizens.GDPR requires organizations that are not based in the EU but handle the data of EU citizens to appoint a European Data Protection Representative. This creates unique representative duties.

7. Regulated Industry Sectors: DPDP Act 2023 has specific data protection standards and considerations; the DPDP Act may contain particular regulations suited to the Indian setting and industry sectors. GDPR offers a unified set of data protection standards that are consistently applicable to all sectors and industries inside the European Union.

8. Cross-Border Transfer Mechanisms: DPDP Act 2023 Subject to certain restrictions and compliance requirements, the DPDP Act permits cross-border data transfers. It outlines the procedures businesses must adhere to when sending data abroad.

GDPR requires organizations to ensure that data transmitted outside the EU is sufficiently protected, which governs cross-border data transfers. It offers particular tools such as binding corporate rules, adequacy rulings, and standard contractual clauses.Cross-Border Transfers: These laws cover cross-border data transfers and set up procedures to guarantee that personal information is sufficiently safeguarded when moved to nations or areas not within their respective jurisdictions. This includes cross-border data protection procedures like binding corporate rules and standard contractual clauses.The General Data Protection Regulation (GDPR) in the European Union and the Digital Personal Data Protection Act 2023 (DPDPA 2023) in India strongly emphasize cross-border data flow. These laws offer instructions on transmitting personal data between jurisdictions while maintaining data security and privacy.

The following paragraphs will discussGDPR and DPDP 2023 cases and cross-border data transfers.

Some scenarios of how Indian laws have specific relevance to Cross Border Transfer are as follows: -

Personal or sensitive data exchanges between India and other countries are called cross-border data transfers in India. These transfers take many different forms. For example, multinational companies may exchange data among their international subsidiaries; Indian companies may use cloud services hosted elsewhere, or individuals may use foreign-provided online services.

India's Legal Frameworks Controlling Cross-Border Data Transfersare as follows: to handle the challenges associated with cross-border data transfers, India has put legislative frameworks in place. The primary statutes consist of:

- The Sensitive Personal Data or Information and Reasonable Security Practises and Procedures in Information Technology Rules of 2011: These regulations require Indian businesses that gather, process, or transfer sensitive personal data to obtain the agreement of the data subjects beforehand. Moreover, they must guarantee that the information is only sent to nations that provide an equivalent degree of data security.
- General Data Protection Regulation (GDPR) Compliance: Indian organizations that interact with data belonging to citizens of the European Union must comply with the stringent requirements of the GDPR. Under strict guidelines that put individual rights and data protection first, the GDPR allows data transfers from the EU to India.
- Data Protection Bill: To replace the current restrictions, India is now working on enacting a comprehensive data protection law. In addition to creating a Data Protection Authority charged with monitoring and guaranteeing compliance, the proposed Data Protection Bill aims to strengthen the regulation of cross-border data transfers.
- "Indian Outsourcing Company": A case involving an Indian outsourcing company that handles personal data for several foreign clients brought attention to how crucial cross-border data transfers are under DPDPA 2023. This organization, which manages client dataworldwide, had to ensure that international data transfer regulations and Indian data protection laws were met. When one of its European clients asked for the transfer of personal

data outside of the European Economic Area (EEA), it encountered difficulties. The Indian outsourcing company had to comply with DPDPA 2023 to permit this transfer, ensuring it fulfilled the data protection standards established by both Indian and European authorities. The case highlighted businesses' need to set up cross-border solid data transfer proceduresand adhere to various jurisdictions' legislative frameworks tobalance global data flows and privacy requirements.

- "Indian Health-Tech Startup": The story of an Indian health-tech business highlighted the DPDPA 2023 framework's considerations for cross-border data transfer. The startup attracted customers from several nations with its creative healthcare application. The firm must send personal health data across borders to comply with the strict rules of the Indian data privacy law while also pursuing global expansion. To accomplish this, the business had to prove its dedication to data security and privacy while safeguarding its global consumers' data rights. The case underscored the necessity for Indian entities to institute well-defined protocols for transnational data transfers, guaranteeing compliance with DPDPA 2023 regulations even as they participate in international data-sharing initiatives.

How does the DPDP Act strengthen the right to privacy under Article 21 in India?

Introduction: -

It is essential to comprehend the meaning of privacy before thoroughly investigating the Right to Privacy. Black's Law Dictionary defines privacy as the "right to be left alone," protecting a person from unwarranted public attention and unwanted intrusion in private topics.According to Article 21 of the Indian Constitution, "No person shall be deprived of his life or personal liberty except by the procedure established by law." Article 21 has come to be interpreted to include all facets of life contributing to a person's meaningful and comfortable living.It's important to note that the Indian Constitution does not explicitly include the Right to Privacy as a Fundamental Right. The case of Kharak Singh, which focused on the validity of laws allowing the surveillance of suspects, served as the starting point for the investigation into this right. The right to privacy was addressed in Justice Subba Rao's minority ruling in this case. The Supreme Court re-examined the right to privacy about Article 19(1)(d) in 1975. Justice Jeevan Reddy concluded in a thorough opinion that Article 21's implicit right to privacy includes the right to be left alone.The Court also decided that if surveillance was extensive and substantially violated someone's privacy, it could interfere with their right to

the freedom of movement protected by Articles 19(1)(d) and 21. Only preventing crime could justify surveillance; this intelligence must come from the suspect's past. The right to privacy was viewed as secondary to state security in the context of anti-terrorism laws, and withholding information essential to preventing crime could not be rejected based on that right. The right to privacy under Article 21 has been explored in various cases.

The DPDP Act 2023 strengthens the right to privacy in India under Article 21 in several ways, as follows:

- Defining personal data broadly: According to the DPDP Act, personal data is any information that can be used to directly or indirectly identify a specific person. This definition of personal data is broader than those found in other data protection legislation, such as the General Data Protection Regulation (GDPR) of the European Union. The DPDP Act definition of personal data includes (A)Biometric Data – which includes data such as fingerprints and facial recognition; (B)Financial Data –which includes bank account numbers and credit/ debit card numbers; and (C) Location Data –this includes data such as GPS coordinates, IP addresses, and cell phone locations.The DPDP Act's requirements for obtaining consent and providing transparency about how the data is used may apply to a company that collects employee biometric information to track their attendance. The DPDP Act's requirements may also apply to a government agency that gathers location data from its citizens to track crime.The DPDP Act's broad definition of personal data represents a significant step towards strengthening privacy protections in India. This comprehensive definition ensures the legal protection of a broader range of personal information as a solid reminder tobusinesses and governments to be cautious when collecting, using, and disclosing personal data.
- Giving individuals the right to access, correct, and delete personal data: The legislation grants people the right to access, amend, and remove their data held by businesses and other entities. Allowing them to confirm the accuracy and currency of their personal information increases individuals' autonomy over that information.To exercise these rights, individuals must formally request to the company or organization in charge of their data. By law, the company or organization must respond to the request immediately by granting access to the person's personal information or carrying out any requested changes or deletions.The DPDP Act established the Data Protection Board (DPB), an independent body tasked with upholding the

Act's provisions and protecting the confidentiality and security of personal data.The DPDP Act is enforced by the DPB using a variety of powers, including the following:

1. Investigating complaints made by individuals about the collection, use, or disclosure of their data.
2. Assessing financial sanctions against organizations that violated the DPDP Act.
3. Requiring businesses to delete any personal information they have stored illegally.

Additionally, the DPB has the power to make regulations that will put the provisions of the DPDP Act into effect.

- Requiring consent for processing personal data: Businesses and other organizations are needed for the DPDP Act to obtain customers' explicit consent before handling their data. According to this, businesses are not allowed to collect, use, or disclose a person's personal information without that person's knowledge and consent.For consent to be legally binding, a person's action must be explicit, affirmative, specific, informed, unambiguous, and voluntary. This demands that people consent voluntarily, free from outside pressure or influence, and clearly understand the information being gathered and how it will be used.

Case laws relating to the right to privacy under article 21 of the Constitution of India w.r.t DPDP Act 2023.

Regarding the recently passed Digital Personal Data Protection Act (DPDP Act) of 2023, there are currently no established legal precedents regarding the right to privacy guaranteed by Article 21 of the Constitution. The Act hasn't yet been subject to any legal challenges in Court because of its novelty.

However, several well-established case laws relating to the right to privacy under Article 21 of the Constitution exist, and some of these may be relevant and applicable to the DPDP Act.

- The Supreme Court of India ruled in a significant legal precedent, Justice K.S. Puttaswamy (Retd.) v. Union of India &Ors. [(2017) 10 SCC 1], that Article 21 of the Constitution protects the fundamental right to privacy. The Court also emphasized that this right has restrictions and may be restricted when there are overriding public interests.
- The K.S. Puttaswamy (Retired) v. Union of India &Ors**. (Aadhaar Case)** [(2019) 1 SCC 1] case is another crucial legal precedent. In this case, the Supreme Court upheld the Aadhaar program's constitutionality while placing stringent restrictions on how the government may use Aadhaar data. The Court ruled that the government was not allowed to collect or use

Aadhaar data for commercial purposes and that people had the right to revoke their consent to use their Aadhaar data.

Recent cases of Data Breach in the Covid-19 Pandemic

Introduction: -Overview of Covid-19 pandemic in India

India, known for its vast and varied population, has experienced a significant and complex impact from the COVID-19 epidemic. India has seen both unique possibilities and challenges as it has navigated the various phases of the outbreak since the first case was recorded in late January 2020. India reacted to the outbreak early on, acting quickly and decisively. The government put in place travel bans, quarantine guidelines, and airport security checks to stop the virus's spread. Despite these early initiatives, the virus spread slowly throughout the country. Among the most important actions was the nationwide lockdown that was put into place on March 24, 2020. This was one of the biggest lockdowns in history, affecting nearly 1.3 billion people and interfering with daily life and economic activity. Even though its goal was to reduce the virus's spread, it presented several difficulties, especially in densely populated urban areas. Social separation and other preventive measures were hard to enforce in overcrowded slums and informal communities.During the pandemic, India's healthcare system was under much strain. It became clear that more hospitals, ventilators, PPE, and medical professionals were required. Hospitals were under pressure due to overworked staff and a lack of essential resources.During the pandemic, India's healthcare system was under much strain. It became clear that more hospitals, ventilators, PPE, and medical professionals were required. Hospitals were under pressure due to overworked staff and a lack of essential resources. An important part of India's reaction to the pandemic was contact tracing and testing. The nation produced its testing kits and increased testing operations. To aid in tracking and containing the virus's transmission, the Aarogya Setu contact tracing app was released. India initiated one of the most considerable vaccination efforts to immunize its sizable population. Vaccines such as Covishield and Covaxin were widely distributed despite logistical obstacles, especially in rural and isolated locations. A deadly second wave of the pandemic struck India in early 2021, with a spike in cases that overtaxed hospitals and healthcare systems. Due to the acute oxygen shortage the country was experiencing, efforts to produce oxygen were intensified both domestically and internationally.India discovered several variants during the pandemic that warranted worry, including the Delta variant, which

is distinguished by its heightened transmissibility. These variations made stopping the virus's transmission difficult and emphasized the value of genetic surveillance.The pandemic severely damaged India's economy, which resulted in job losses, company closures, and severe financial hardship, especially for the vulnerable and informal workers. A humanitarian crisis was created when the lockdowns caused a large-scale migration of migrant laborers from cities to their rural villages. Public health efforts to increase knowledge of preventive measures like mask use, hand cleanliness, and social distancing were part of India's response.Ensuring fair access to vaccines for every group in the population, however, continued to be complicated. Despite its difficulties, India was a crucial player in the international effort to contain the pandemic. The nation demonstrated its dedication to global collaboration in health cooperation by participating in programs like COVAX and donating vaccines to other countries. India demonstrated resilience, flexibility, creativity, and research in reacting to the COVID-19 epidemic. The country's primary priorities are strengthening the healthcare system and preparing for future health emergencies. The pandemic's effects demonstrate India's capacity to adjust and react to changes as the country fights the virus and moves toward recovery.

Impact of COVID-19 on Digital Personal Data Protection in India: -

- Increased dependence on Digital Technologies: The pandemic hastened the acceptance of digital technologies in commerce, education, healthcare, and distance employment. As a result, the amount of personal data created and handled online increased dramatically. Data protection consequently becomes much more critical.
- Security Concerns with Data: Data breaches and cyberattacks were increasingly likely as more people used digital platforms for diverse purposes and worked from home. Organizations and people have made it their top responsibility to protect personal data.
- Awareness of Data Privacy: The pandemic increased people's understanding of the value of data privacy. People started to want more transparency and control over personal information as they were more aware of the "data" they were sharing online.
- Policies for "Bring Your Device" (BYOD) and Remote Work: Many companies have adopted BYOD and remote work policies, which present data security issues. It became a worry to ensure that personal data on employees' devices is protected.

- Data Processing for Contact Tracing:To track and stop the virus's propagation, contact tracing operations frequently need the gathering and processing personal data. This made some wonder if gathering data was necessary and proportionate.
- Debate about Data Localization: The pandemic raised awareness of this problem. The management and storage of data by international corporations may be impacted by the Indian government's consideration of data localization laws for specific categories of personal data.
- Digital Surveillance: To monitor and control the epidemic, certain governments and organizations employ technologies and methods for digital surveillance. Public safety was the primary motivation behind this "action"; however, privacy and monitoring issues were also discussed.
- Data Breaches and frauds: Cybercriminals exploited the pandemic to their advantage, launching COVID-19-related data breaches and frauds. This emphasized the necessity of adequate data protection procedures and cybersecurity defenses.

Case studies of privacy violations and COVID-19 data breaches in India:-

Introduction: -The GDPR and DPDPA 2023 are robust frameworks for data protection, as shown by their comparative study. The necessity of these rules' stringent enforcement and ongoing vigilance is highlighted by their use in actual situations, such as data breaches during the COVID-19 outbreak in India. The incidents covered show how important DPDPA 2023 is for protecting personal information and making organizations responsible for data breaches. In an increasingly digital world, the study highlights the necessity of ongoing improvements to data protection safeguards and calls for a global effort to harmonize data protection standards.Furthermore, to strengthen data protection and privacy laws, India was in the process of passing the Digital Personal Data Protection Act 2023 (DPDPA).

- **The Aarogya Setu App Data Breach[8]**

Facts - India's efforts to contain the COVID-19 epidemic were greatly aided by the April 2020 debut of the Aarogya Setu mobile application. In addition to helping users determine their risk of virus infection, it functioned as a contact tracing and health monitoring tool.

[8]Mehendi Mazumdar, Arogya Setu and Cowin: Ethical and Legal Issues, 2 Indian J. Integrated Research in Law 462 (2022)https://ijirl.com/wp-content/uploads/2022/01/AROGYA-SETU-AND-COWIN-ETHICAL-AND-LEGAL-ISSUES.pdf

However, a significant data breach that affected the Aarogya Setu app has caused controversy, underscoring the significance of India's data protection legislation.

Purpose- The app aims to track and share information regarding COVID-19 instances, encourage self-evaluation, and make contact tracking easier. It gathered user data, such as location and health-related data.

Collection of Data- The app gathered various data, such as location information, Bluetooth proximity information, and health information based on self-evaluation.

The Data Breach of the Aarogya Setu App- The Breach Discovery: Elliot Alderson, an ethical hacker, found a security flaw in the Aarogya Setu app in May 2020. An attacker could access a user's personal information without authorization because of this vulnerability.It highlighted the significance of accountability and adherence to data protection legislation.

Data Protection Authority- The event clarified how important it is for the Authority to look into and resolve data protection violations.

Public Perception and Trust-The Aarogya Setu app data breach questioned the public's perception of government-led digital initiatives. Preserving public trust in these applications requires ensuring data is protected and dealing with breaches.

Conclusion- The Aarogya Setu app data breach highlighted the importance of India's data protection legislation, especially the DPDPA 2023, in protecting people's personal information. Although the hack revealed vulnerabilities in the app's data security, it also highlighted the significance of accountability, promptness, and openness in handling data breaches. It acts as a case study for how businesses and the government can prioritize cybersecurity and data protection in digital efforts, mainly when there is a public health emergency.

- **Data Breach at a Leading E-commerce Company (Mobikwik)**

Facts- Data breaches remain a problem in the digital age due to the rising sophistication of cyberattacks. This case study explores a significant data breach that occurred at a prominent Indian e-commerce company, and it looks at how the nation's data protection laws were crucial in handling the situation and guaranteeing the security of people's personal information.One of the top e-commerce businesses in India experienced a significant data breach in 2021. A cybersecurity researcher discovered a database on the dark web that contained sensitive client information, which led to the detection of the hack.

Type of Data Exposed- A significant quantity of personal data, including user names, physical addresses, telephone numbers, email addresses, and even order histories, were made public by the hack. Information of this kind might be used for fraud, identity theft, or other nefarious purposes.

Legal consequences- Thee-commerce company faced severe repercussions from the data breach. After learning about the intrusion, authorities launched an inquiry and carefully examined the business's security protocols and data protection procedures.The company was required to report the breach tothe impacted parties. A key component of data protection regulations is this timely notification, which enables people to take the appropriate precautions to safeguard their privacy and personal information.

Conclusion, Recommendations, and References

Conclusion: - Two of the most extensive data protection regulations in the world are the General Data Protection Regulation (GDPR) and the Digital Personal Data Protection Act (DPDP Act). Both laws regulate the gathering, handling, and cross-border transmission of personal data to preserve peoples' privacy.Regarding cross-border data transfers and the right to privacy, this research paper has compared and contrasted the DPDP Act and GDPR. The research has shown that while there are some parallels between these two laws, there are also significant differences.The right to privacy is acknowledged as a fundamental entitlement by the DPDP Act and GDPR. They differ, nevertheless, in terms of how they defend this right. The GDPR, for example, has a more expansive definition of personal data than the DPDP Act. It gives data subjects more power over their data, including the ability to requestthe deletion of their personal information.Contrary to the GDPR, the DPDP Act does not impose a general ban on cross-border data transfers. Instead, it enables international data transfers to nations that have been given the Central Government's seal of approval. Contrarily, the GDPR forbids data transmission across international borders to countries outside the European Economic Area (EEA) unless those nations adhere to strict guidelines for appropriate data protection.The research also delves into the implications of these laws for businesses and organizations operating across multiple jurisdictions. Entities subject to the GDPR must take additional measures to ensure compliance with cross-border data transfers. Those adhering to the DPDP Act enjoy more flexibility but must still meet the Act's requirements. In conclusion, India has enormously advanced data protection via the DPDP

Act. The report does point out several areas where it may be improved, like the addition of more apparent enforcement mechanisms and a stronger focus on privacy protection in the context of international data transfers.

Recommendations: -To boost the DPDP Act 2023, we recommend

- Introducing an explicit system of checks and balances.
- Improving the privacy protection for international data transfers.
- Clarifying the definition of personal data.
- Empowering the data subjects with more control over their data.

References: -

1. Aditya Bashambu& Lavanya Chetwani, Critical Analysis: Digital Personal Data Protection Bill 2022, 3 Jus Corpus L.J. 519 (2022). https://www.juscorpus.com/wp-content/uploads/2023/01/108.-Adiyta-Bashambu-and-Lavanya-Chetwani.pdf
2. Kuner, Christopher, The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards (November 20, 2021). National Law Review of India, vol. 33 no. 1 (2021), Available at SSRN: https://ssrn.com/abstract=3964672
3. Adv. Ashwini Kumar, The Digital Personal Data Protection Bill 2022 in Contrast with the EU General Data Protection Regulation: A Comparative Analysis, 5 IJFMR 3 (2023). https://www.ijfmr.com/papers/2023/2/2534.pdf
4. Cross-Border Transfer of Personal Data under the Digital Personal Data Protection Bill 2022: A Comparative Analysis, TSAARO (Jan. 5, 2023), https://tsaaro.com/blogs/cross-border-data-transfers-under-the-digital-personal-data-protection-bill-2022/
5. Sinha, Amber. "India's Data Protection Framework Will Need to Treat Privacy as a Social and Not Just an Individual Good." Economic and Political Weekly, vol. 53, no. 18, May 5, 2018, pp. 18-21
6. Mehendi Mazumdar, Arogya Setu, and Cowin: Ethical and Legal Issues, 2 Indian J. Integrated Research in Law 462 (2022) https://ijirl.com/wp-content/uploads/2022/01/AROGYA-SETU-AND-COWIN-ETHICAL-AND-LEGAL-ISSUES.pdf