INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBER INCIDENT RESPONSE AND DATA BREACH NOTIFICATIONS LAWS: A COMPARATIVE STUDY OF INDIA, THE UNITED STATES, AND THE EUROPEAN UNION

AUTHORED BY - AKANSHA BARUA
II SEMESTER, LL.M
IILM UNIVERSITY, GREATER NOIDA

CO-AUTHOR - HARDIK MALIK
Assistant Professor
IILM UNIVERSITY, Greater Noida

1. ABSTRACT

In today's digital world, cyber-attacks and data breaches are happening more and more, which affects governments, companies, and people. Because of this, many countries have made laws to deal with cyber incidents and require businesses to report data breaches within a specific time. This research paper looks at the laws about handling cyber incidents and reporting data breaches in three areas: India, the United States, and the European Union.

The study explains how different regions handle reporting data breaches, including their rules, time limits, and how they enforce them. In the European Union, there is a strong and organized system based on GDPR[1]. Companies there have to report breaches quickly and follow strict guidelines. In the United States, there are different laws in various states and industries, so the system is not very consistent. India has a centralized system through CERT-In, where companies need to report cyber incidents quickly, but the overall data protection laws in the country are still being developed.

The paper compares these systems to understand their strengths and weaknesses. It also talks about problems such as different rules in various countries, trouble dealing with cyber-attacks that happen across borders, and issues companies face when following laws. At the end, the paper recommends that countries team up to make clearer and better cyber laws, which could help make the world safer online.

[1] General Data Protection Regulation (GDPR), available at: https://gdpr-info.eu/ (last visited on - 14 April 2026).

ISSN: 2582-6433

KEYWORDS: Cyber Incidents, Data Breaches, GDPR, Data Protection

2. INTRODUCTION

In today's digital world, most activities rely on computers, internet services, and online platforms. As technology becomes more popular, cyber incidents and data breaches are happening more often. These incidents occur when important or personal data is viewed, taken, or shared without permission. This can cause damage to individuals, businesses, and even governments.

To handle this issue, many countries have made rules that ask organizations to act fast during cyber-attacks and to tell the people affected and the government if there's a data breach. These rules are called cyber incident response and data breach notification laws. The main goal is to make sure there are quick action, honesty, and safety for personal information.

Different countries have their own ways of dealing with these issues. The European Union has a strong and consistent system based on the General Data Protection Regulation (GDPR), which requires strict rules for reporting data breaches. The United States has a system that varies by state and industry, so the rules are not the same everywhere. India uses the Information Technology Act, 2000[2], which gives the basic structure for cyber law and data protection, but its full data protection system is still being developed.

3.)NEED, RELEVANCE AND IMPORTANCE OF STUDY NEED OF THE STUDY

As digital technology continues to develop quickly, cyber incidents and data breaches are happening more often. Personal and sensitive information is always in danger, so it's important to examine how laws handle responses to cyber incidents and require notification of data breaches. It's also essential to compare the legal systems of India, the United States, and the European Union to spot areas that need improvement and strengthen current rules.

RELEVANCE OF THE STUDY

This study is relevant because protecting data and keeping it secure are huge issues around the world. Companies run their operations in many countries, but each place has its own set of

[2] Information Technology Act, 2000, India, available at: https://www.indiacode.nic.in/handle/123456789/1999 (last visited on - 14 April 2026).

ISSN: 2582-6433

rules. By comparing these rules, we can better understand how they affect businesses, people, and governments. This kind of analysis is also helpful for lawyers, people who make laws, and researchers who study cyber law and data protection.

IMPORTANCE OF THE STUDY

This study is significant because it shows the pros and cons of various legal systems. It helps spot problems like inconsistent laws, issues that come up when countries work together, and difficulties in following rules. The study can help create better policies and push for more cyber laws around the world, which can result in stronger data protection and more effective cybersecurity measures.

4.)STATEMENT OF PROBLEM

There isn't a single, agreed-upon set of laws around the world for handling cyber incidents and notifying about data breaches. Countries like the European Union, the United States, and India have their own rules, timeframes, and ways of enforcing these laws. This lack of uniformity leads to different requirements for reporting and creates challenges for companies that work in multiple countries. Because of this, there are often delays in reporting breaches, confusion about the legal rules, and problems in keeping personal data safe. All of this makes it hard to coordinate cybersecurity efforts on a global level.

5.)LITERATURE REVIEW

The research on how to respond to cyber incidents and the laws about notifying data breaches shows that protecting data has become a major issue because of how quickly digital technology is growing and how serious cyber threats are. Most experts agree that different countries have created their own legal systems to handle data breaches.

In the European Union, studies point out that the GDPR is a strong and well-organized law with clear rules about reporting breaches and strict enforcement.

In the United States, the research focuses on a system that is split between state laws and rules specific to certain industries, which leads to uneven protection.

In India, studies show that the IT Act of 2000 provides some basic legal structure, but it still doesn't have a detailed and consistent way to handle data breach notifications.

Overall, the research shows that while there has been progress around the world, there is still a need for more consistent and unified cyber laws to properly deal with cyber incidents that

ISSN: 2582-6433

happen across borders.

6.)RESEARCH GAP

There isn't much detailed comparison of how countries handle responding to cyber incidents and notifying about data breaches in the European Union, the United States, and India, especially when it comes to how well these laws work in practice, how they are enforced, and the actual problems that come up in real situations.

7.)RESEARCH OBJECTIVES

1. To examine and compare the laws that control how cyber incidents are handled and how data breaches are reported in the European Union, the United States, and India.
2. To understand how these legal systems differ, the obstacles they face, and how well they work in making sure personal data is reported on time and protected properly.

8.)SCOPE AND LIMITATIONS

SCOPE

This research focuses on the legal frameworks surrounding cyber incident response and data breach notification in the European Union, the United States, and India. It looks at key legislation such as the GDPR, state-level laws in the U.S., and the Information Technology Act, 2000. The study also involves a comparison of notification deadlines, enforcement methods, and regulatory setups. It helps in understanding how different legal systems handle cyber incidents and safeguard personal data.

LIMITATIONS

This study relies solely on secondary sources such as laws, regulations, and online resources, and does not involve any primary data collection or interviews. It is restricted to three specific jurisdictions and does not encompass all countries globally. The research primarily focuses on legal frameworks and does not provide an in-depth analysis of technical cybersecurity tools or industry-specific practices.

9.)RESEARCH METHODOLOGY

This study uses a doctrinal and comparative approach, relying on secondary sources like statutes, regulations, articles, reports, and online legal resources, to examine and compare the

ISSN: 2582-6433

laws related to responding to cyber incidents and notifying data breaches in the European Union, the United States, and India.

10.) HYPOTHESIS

The European Union has a more efficient and consistent data breach notification system than the United States and India, which have fragmented and developing legal frameworks.

11.) EVOLUTION OF DATA BREACH NOTIFICATION LAWS

The development of data breach [3]notification laws is closely linked to the rapid growth of digital technology, internet usage, and large-scale data storage. In the past, there were no clear rules that made companies tell people about cyber-attacks or data leaks. But as cybercrime became more common and personal information started being kept online in large amounts, it became clear that there needed to be laws requiring companies to share this information with people.

In the early 2000s, the United States took an important step in this area when California passed the first data breach notification law in 2002. This law made it necessary for companies to let people know if their personal information was accessed or stolen during a security incident. Soon after, many other states in the US created their own similar laws, which led to a system where each state has its own rules about how to notify people about data breaches.

At the international level, the need to protect personal data became much more important as global digital platforms grew. In 2016, the European Union created a more organized and consistent way to handle data protection through the General Data Protection Regulation (GDPR). This law required all member countries to report data breaches and set a strict rule that they must notify affected people within 72 hours. This change showed a big move towards a common global standard for protecting personal data.

In India, rules about data breaches started to form slowly through the Information Technology Act of 2000, which gave the first legal structure for cyber security and protecting data. As time went on, the need for better rules led to improvements in how cyber incidents are reported, especially because cyber threats became more common in the country.

Today, data breach laws have moved from being almost non-existent to becoming an important

[3] Evolution of data breach, available at: https://www.procurri.com/knowledge-hub/data-breaches-from-past-to-future-how-data-breaches-evolved-their-costs-and-how-to-mitigate-risks/ (last visited on 16 April 2026)

ISSN: 2582-6433

part of modern privacy and cyber security rules. Most countries now see the value in quickly reporting breaches as a way to keep people safe and build trust in digital systems.

12.) CONCEPTUAL FRAMEWORK

12.1 MEANING OF CYBER INCIDENT

A cyber incident [4]happens when a computer system, network, or digital data is targeted, accessed without permission, or disrupted. This can involve things like hacking, using harmful software, tricking people to get information, holding data for ransom, or any kind of unwanted access to computer systems.

12.2 MEANING OF DATA BREACH

A data breach occurs when someone gets access to personal or private information without being allowed to. This can happen if the security measures in place are not working properly or are used in the wrong way, causing details like names, passwords, money information, or identification numbers to be shared or taken.

12.3 MEANING OF PERSONAL DATA

Personal data refers to any information that can be used to identify someone either directly or through some other means. This includes things like a person's name, address, email address, phone number, identification numbers, financial details, or any other type of information that can help recognize a particular individual.

12.4 WHAT IS CYBER INCIDENT RESPONSE?

Cyber incident response is when you find out, deal with, and handle a cyber-attack or a security problem. It involves steps to spot the issue, stop or limit the harm, look into what happened, and fix the systems that were affected.

12.5 MEANING OF DATA BREACH NOTIFICATION

Data breach notification is a law that requires companies to tell people who were affected and the proper government agencies when a data breach happens. This helps inform individuals that their personal or important information might have been viewed, taken, or shared without their permission.

[4] Richard Bejtlich, "The Practice of Network Security Monitoring: Understanding Incident Detection and Response", 24 Journal of Digital Forensics, Security and Law 15 (2019).

ISSN: 2582-6433

12.5.1 WHY NOTIFICATION LAWS ARE NEEDED

Data breach notification laws [5]are important because they make sure people and companies know right away if personal information has been shared or taken. If there are no such laws, businesses might not tell people about breaches or might wait too long to report them, which can make things worse.

These laws let people act quickly, like changing passwords or checking their bank accounts, to stop problems like identity theft or money fraud.

They also help keep things open and honest, making companies more careful about keeping data safe.

13.) EUROPEAN UNION LEGAL FRAMEWORK

The European Union has a very detailed and organized system for handling cyber incidents and informing about data breaches. The EU places a strong emphasis on protecting people's personal information; making sure things are open and clear, and holding organizations responsible when a cyber-problem happens.

The main law that covers this is the General Data Protection Regulation, or GDPR. According to GDPR, a "personal data breach" is any event that results in the accidental or illegal destruction, loss, changes, sharing without permission, or unauthorized access to personal data. Companies that control personal data, called data controllers, must evaluate the risk of a breach and act quickly once they find out about it.

If there's a data breach that could harm people's rights and freedoms, the company must tell the proper authority within 72 hours after they find out about the breach. If the breach is serious, the company also needs to warn the people affected as soon as possible. This helps people take fast actions like changing their passwords, stopping their accounts from being used, or keeping an eye on their money.

The GDPR also requires data processors to quickly inform data controllers about any data breaches, making sure that everyone involved in handling data is responsible. Each EU country has its own independent authority that checks compliance and can impose big penalties, like large fines, if the rules are not followed.

Besides GDPR, the EU has also created the NIS2 Directive[6]. This new rule makes cybersecurity

[5] Regulation (EU) 2016/679 (General Data Protection Regulation), available at: https://gdpr-info.eu/art-33-gdpr/ (last visited on 16 April 2026).

[6] Directive (EU) 2022/2555 (NIS2 Directive), available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (last visited on 16 April 2026)

ISSN: 2582-6433

stronger in key areas like banking, energy, transportation, healthcare, and digital systems. NIS2 is focused on protecting networks and information systems. Companies must follow strict rules to manage risks and report big cyber-attacks to their country's authorities quickly. It also helps EU countries work together better when there are serious cyber threats.

The EU's legal system [7]is seen as one of the best globally because it has tight rules for protecting data, clear rules about reporting issues, strong ways to enforce these rules, and a united approach to managing cybersecurity in all the countries that are part of the EU.

14.) UNITED STATES LEGAL FRAMEWORK

14.1 NO SINGLE FEDERAL LAW

In the United States, there isn't one single law that covers all data breach situations nationwide. Instead, each state has its own rules about how and when companies must report data breaches. Because of this, the requirements vary from state to state.

Each state has its own way of defining what a data breach is and how quickly companies must inform people. This makes it harder for businesses that work in multiple states, as they have to follow different rules at the same time.

In addition to state laws, some industries are governed by federal laws[8], like healthcare and financial services. But these laws only apply to specific areas and don't create a single national standard. Overall, the US system is seen as scattered because there isn't one common law that applies to all data breaches across the country.

14.2 STATE-WISE DATA BREACH NOTIFICATION LAWS

In the United States, there isn't one federal law that covers all the states when it comes to data breaches. Instead, each state has its own rules about when companies must inform people if their personal information is exposed. Because of this, the laws vary from state to state.

All 50 states, plus the District of Columbia and some U.S. territories, have these laws. Even though the goal of these laws is the same, there are differences in what counts as personal information, how quickly companies must notify people, and what information they need to report. This means that businesses that operate in multiple states might have to follow different rules in each place.

[7] EU legal system available at: https://commission.europa.eu/law/law-making-process/types-eu-law_en (last visited on 16 April 2026)

[8] Reed Abelson, "Health Data Breaches Raise Concerns Over Patient Privacy", The New York Times, March 15, 2023.

ISSN: 2582-6433

Most state laws in the US require companies to inform people whose data was involved in a breach as soon as possible, without unnecessary delays. A few states also ask businesses to report the breach to the attorney general or other government agencies. California was the first state to pass such a law in 2002, and since then, other states have started to create similar rules. Overall, the US has a system where each state has its own version of the law, which makes the process for handling data breaches varied and not entirely the same across the country.

14.3 SECTOR-BASED DATA BREACH LAWS (HEALTH AND FINANCE)

In the United States, rules about data breaches come from both state laws and special federal laws that apply to certain industries like healthcare and finance. These laws help keep personal information safe in areas that are closely watched.

In the healthcare area, there's a law called HIPAA that handles how patient information is protected and what to do if there's a breach. HIPAA says that hospitals, insurance companies, and other related groups must tell the people whose information was affected and the proper authorities if their medical data is stolen or exposed. This helps make sure medical records and patient privacy are kept secure.

In the financial sector, data security is covered by laws like the Gramm-Leach-Bliley Act (GLBA). This law tells financial companies to protect their customers' financial information and use security steps to stop people from getting into it without permission. If there is a data leak, the companies have to let their customers know and fix the problem.

Even though these rules are strong for their specific areas, they don't create one big national rule for all data breaches. So they work together with state laws, which make the US system for reporting data breaches a bit scattered and not fully connected.

15.) INDIAN LEGAL FRAMEWORK

15.1 INFORMATION TECHNOLOGY ACT, 2000

The main law that controls cyber activities and data protection in India is the Information Technology Act, 2000 (IT Act). It sets up the basic rules for handling cyber-crimes, illegal access to computer systems, and protecting electronic data.

The IT Act also has rules about liability when there is a data breach. Section 43A says that companies dealing with personal data must use proper security measures. If they fail to do so and a data breach happens, they can be held responsible. Section 72A explains the penalties for sharing personal information without permission.

The Act also gives legal recognition to electronic records and digital transactions, which helps

ISSN: 2582-6433

control online activities. However, it does not have a detailed and clear system for notifying about data breaches, like the GDPR in the European Union. Instead, India uses rules specific to different sectors and government instructions for reporting cyber incidents.

Overall, the IT Act, 2000 is the base of India's cyber law, but it is still changing to deal with new challenges in data protection and cyber security.

16.) COMPARATIVE ANALYSIS

16.1 NOTIFICATION TIMELINES

The timeframes for notifying about cyber incidents and data breaches vary a lot between the European Union, the United States, and India. In the European Union, the GDPR requires companies to inform the proper authority about a personal data breach within 72 hours after they find out about it. This set time limit helps ensure regulators can act quickly and reduce potential harm early on.

In the United States, there is no single national timeline for reporting. Each state has its own rules, but most require that notifications be given without unnecessary delay. This allows some flexibility but also leads to differences in how things are handled in different areas.

In India, CERT-In sets guidelines that require organizations to report certain cyber incidents very quickly, usually within hours of detecting them. This makes India's approach stricter when it comes to how fast reports must be made, but it only applies to specific types of cyber incidents, not all data breaches.

16.2 ENFORCEMENT BODIES

The enforcement of cyber incident response and data breach notification laws differs across the European Union, the United States, and India based on their regulatory structures.

In the European Union, data protection is enforced by Data Protection Authorities [9](DPAs) in each country. These authorities check if companies follow the GDPR, look into data breaches, and give heavy fines to those who don’t comply.

In the United States, data enforcement is handled by two main groups: the Federal Trade Commission (FTC) and State Attorneys General. The FTC takes care of consumer protection at the national level, while the State Attorneys General enforce rules specific to their states. This setup makes the enforcement process both shared and spread out across different states.

[9] Natasha Lomas, “Europe’s Data Protection Authorities Step Up GDPR Enforcement”, TechCrunch, May 25, 2023.

ISSN: 2582-6433

In India, data protection is mainly enforced through the Information Technology Act, 2000. The Ministry of Electronics and IT (MeitY) and the Indian Computer Emergency Response Team (CERT-In) are responsible for monitoring and responding to cyber incidents. However, the enforcement system in India is more focused and still growing compared to the systems in the EU and the US.

16.3 SCOPE OF "DATA BREACH"

The scope of a data breach means how big the problem is and how much damage it can cause. It tells us how serious the breach is and what steps need to be taken legally after it happens.

A data breach can include different kinds of information, like personal details such as names, addresses, and emails, financial information like bank or credit card details, or sensitive records such as health information or ID data.

The size of the breach depends on how much data was involved and how many people were affected.

The scope also looks at what caused the breach, like whether it was a mistake, carelessness, or a deliberate attack by someone with bad intentions. It also checks if the data was just viewed or if it was used improperly or shared with others.

Knowing the scope is important because it helps decide how bad the harm is, how quickly people need to be told, and what legal actions are required based on different cyber laws.

16.4 PENALTIES

Penalties for not following rules about responding to cyber incidents and reporting data breaches differ depending on the country and the severity of the violation.

In the European Union, the GDPR imposes very strict penalties for not reporting data breaches or not following proper data protection measures. These fines can be as high as €20 million or 4% of the company's global annual revenue, whichever is higher. This makes the EU's system one of the toughest in the world.

In the United States, penalties can vary because laws are different in each state and industry. Companies might get fined by groups like the FTC, face penalties from their state governments, and also be sued by people who were harmed. The amount of money they have to pay usually depends on how much damage was done.

In India, the penalties under the Information Technology Act, 2000 are not very high compared to other places, but they are still quite big. Companies might have to pay money if they fail to protect personal data properly, and they could also face fines if they share private information

ISSN: 2582-6433

without permission.

17.) ROLE OF REGULATORY AUTHORITIES

Regulatory bodies are important in making sure companies follow rules about responding to cyber-attacks and informing people about data breaches. They help organizations meet legal standards, keep personal information safe, and report any data leaks quickly.

In the European Union, each country has its own independent Data Protection Authority that checks if companies are following the GDPR. These authorities look into data breaches, provide guidance, and can fine companies heavily if they break the rules.

In the United States, the Federal Trade Commission (FTC) and State Attorneys General are mainly responsible for enforcing rules. They step in when companies don't keep consumer data safe or act unfairly.

In India, the main laws and rules for regulating the internet and handling cyber issues are based on the Information Technology Act, 2000. There are also government groups that focus on cybersecurity and technology. These groups make sure that people follow the rules and deal with any problems related to cyber-attacks or security issues.

17.1 EU: DATA PROTECTION AUTHORITIES (DPAs)

In the European Union, Data Protection Authorities [10](DPAs) are separate public organizations that make sure data protection laws are followed according to the General Data Protection Regulation (GDPR). Each country in the EU has its own DPA, which checks that companies follow GDPR rules, like managing personal information correctly and reporting data breaches quickly. DPAs also look into complaints from people, check if companies are following the rules, and take steps against those who break data protection laws.

They also have the power to enforce rules strongly, like giving warnings, telling companies to change how they handle data and charging big fines if they don’t follow the rules. This makes DPAs an important part of the EU’s strict and effective data protection system.

17.2 US: FTC + STATE ATTORNEYS GENERAL

In the United States, the main groups that enforce laws related to data breaches and privacy are the Federal Trade Commission (FTC) and the state attorneys general.

[10] European data protection board, available at: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en (last visited on 16 April 2026).

ISSN: 2582-6433

The FTC is the main federal organization that protects consumers. It steps in when companies don't properly protect people's personal information or act in ways that are unfair or misleading. However, the FTC doesn't have a specific law that applies to all data breaches nationwide. Instead, it uses its broader powers to protect consumers from unfair practices.

Besides the FTC, state attorneys general also help enforce laws that require companies to report data breaches. They can look into breaches, sue companies that don't follow the rules, and make sure businesses meet their state's requirements.

17.3 INDIA: MEITY + CERT-IN

In India, cyber security governance and handling of security incidents are mainly managed by the Ministry of Electronics and Information Technology (MeitY) and the Indian Computer Emergency Response Team (CERT-In). MeitY is the central government department that creates policies and rules for information technology and cyber security. It is also responsible for setting up the legal and policy structure for digital governance in the country.

CERT-In, which works under the Ministry of Electronics and Information Technology, is the national body that deals with cybersecurity issues. It gathers reports about cyber incidents, sends out warnings and guidance, and helps organize responses to significant cyber threats across the country.

18.) CHALLENGES IN CYBER INCIDENT RESPONSE LAWS

a) **Lack of uniform global laws**- Different countries have their own cyber laws, and there are no rules worldwide. This makes it hard for companies that work in multiple countries to know what rules to follow.
b) **Different definitions of data breach**- Different places have their own way of defining what a "data breach" is, which makes it hard to follow the same rules for compliance everywhere.
c) **Cross-border cyber incidents**- When data is stored in multiple countries, it becomes difficult to determine which law will apply.
d) **Delay in reporting breaches**- Organizations often delay reporting due to fear of penalties or reputational damage.
e) **High compliance burden**- Companies that work in several areas have to follow different rules in each place, which makes things more expensive and harder to manage.
f) **Fast changing technology**- Cyber threats change faster than laws, which mean rules become old and not useful quickly.

ISSN: 2582-6433

19.) CASE STUDIES

a) **Facebook–Cambridge Analytica Scandal (EU/Global Impact) -** This case showed how personal data of millions of users was used improperly without their permission. It revealed poor ways of protecting data and resulted in tougher enforcement of GDPR rules in the European Union. It emphasized the need for strict privacy and clear rules about how data is handled.

b) **Equifax Data Breach (United States) -** In 2017, Equifax, a big company that handles credit reports, had a huge security problem that affected millions of people. Personal details such as Social Security numbers and financial information were made public. This incident highlighted how poor cybersecurity and slow action can have big consequences, especially when the legal system is not unified.

c) **AIIMS Ransomware Attack (India) -** In 2022, India's top medical college, AIIMS, was hit by a ransomware attack. This caused problems with their services and showed weaknesses in how healthcare systems protect computer data. It showed that India needs better ways to respond to cyber-attacks and stronger rules to keep patient information safe.

20.) CRITICAL ANALYSIS

A comparison of how countries handle cyber incidents and data breaches in the European Union, the United States, and India reveals big differences in their laws, how strictly they are enforced, and how well they work in practice.

The European Union's GDPR system is the most organized and efficient because it sets the same rules for all member countries, requires reports to be filed within 72 hours, and enforces these rules with serious fines. But these strict rules can sometimes be a big challenge for companies, especially smaller ones.

The U.S. system is more flexible but also very split up. State laws and rules for different industries let things change easily, but there’s no one national law. This lack of a single law causes differences and mix-ups for companies that work in many states. It lowers the overall consistency and makes following the rules harder.

In India, the legal system is still growing. The Information Technology Act, 2000 gives some basic rules, but there isn't a full law for reporting data breaches like the GDPR. Although some areas are getting stricter with enforcement, the system still doesn't have clear and consistent rules.

ISSN: 2582-6433

21.) CONCLUSION

Cyber-attacks and data leaks are now a big problem around the world because more and more people rely on digital technology. This study explains that various countries have created different laws to handle these issues.

The European Union has a strong and consistent system based on the GDPR, with clear rules about when to report issues and strong tools to enforce those rules. The United States has a different system where laws vary by state and industry, leading to some differences but also giving more room for different approaches. India is still building its legal framework using the Information Technology Act from 2000 and is slowly improving its laws to better protect against cyber threats.

Overall, the comparison shows that there isn't one single global rule for how to handle cyber incidents and report data breaches. But it also shows that there's a strong need for more teamwork and agreement between countries to deal with cyber threats that cross borders and to better protect personal information around the world.

22.) RECOMMENDATIONS

Based on the comparison of how countries handle cyber incidents and data breaches in the European Union, the United States, and India, it is suggested that there should be more agreement on cyber laws worldwide to better deal with data breaches that happen across borders. India should create a clear and detailed system for reporting data breaches, similar to the GDPR, to make things more transparent and hold organizations accountable. The United States should think about having a single national law instead of the many different rules set by each state. Also, there needs to be stronger ways to make sure these laws are followed, and better teamwork between the agencies that regulate data. Companies should also be encouraged to use better technology and provide regular training to improve how they respond to cyber incidents. In the end, better international teamwork, clear rules, and proactive security steps are key to making data protection and cybersecurity stronger around the world.