



LegalOnus

Aequitas Sequitur Legem

“A QUALITY
INITIATIVE FOR
LEGAL
DEVELOPMENT,
UNDERTAKEN
BY
LEGALONUS”



LEGALONUS LAW JOURNAL
ISSN: 3048-8338



www.legalonus.com Email: journal@legalonus.com

About Us - LegalOnus Law Journal (LLJ)
ISSN: 3048-8338

LegalOnus Law Journal (LLJ) is a monthly, peer-reviewed, online academic journal dedicated to advancing legal scholarship. We provide an interactive platform for the publication of short articles, long articles, book reviews, case comments, research papers, and essays in the field of law and multidisciplinary issues.

Our mission is to enhance the level of interaction and discourse surrounding contemporary legal issues. By fostering a dynamic environment for discussion, we aim to elevate the quality of legal scholarship and become a highly cited academic publication.

We invite quality contributions from students, academics, and professionals across the industry, the bar, and the bench. Join us in our commitment to advancing legal knowledge and practice.

Disclaimer for LegalOnus Law Journal (LLJ)
ISSN: 3048-8338

All content published in the LegalOnus Law Journal (LLJ) is the intellectual property of their respective authors and contributors. The authors' copyright of articles, reviews, and other contributions remains.

Reproduction, redistribution, or commercial use of any materials from LLJ is strictly prohibited without prior written permission from the copyright holder and LLJ. The opinions expressed in the articles are those of the authors and do not necessarily reflect the views of LLJ or its editorial board.

LLJ and its editorial team are not responsible for any copyright infringements or legal issues arising from unauthorized use of the journal's content. For permissions, queries, or copyright concerns, please contact the LLJ editorial team at journal@legalonus.com. By accessing and using LLJ content, you agree to comply with this disclaimer and all applicable copyright laws.

Ayush Chandra

Publisher, Managing Director, & Founder



Mr. Ayush Chandra is the Publisher, Managing Director, and Founder.

He pursued an extensive legal education and practical experiences, significantly enriching his expertise. He graduated with first-division marks in a 5-year integrated BA-LLB course from Amity University. His education provided a solid foundation in legal studies. His internships included the District Legal Services Authority at a lower court, the Allahabad High Court under a seasoned advocate, and the Supreme Court of India.

These experiences deepened his understanding of the legal system, honing his analytical skills and expertise in drafting and pleading.

ayush.chandra@legalonus.com

+91 9140433246

Editorial board

Prof. (Dr.) Jay Prakash Yadav

Senior Chief Editor

Prof., and Director, Amity

Law School

Amity University,

Gurugram, Haryana



Dr. Radha Ranjan

Editor-in-Chief

Assistant

Professor,

Amity University,

Patna, Bihar.



Mr. Rachit Sharma
Editor-in-Chief
Assistant Professor
IILM University,
Greater Noida

Dr. Anandh Kumar V
Editor-in-Chief
Assistant Professor
SRM School of Law,
SRMIST, Tamil Nadu





Megha Middha
Editor-in-Chief
Research Scholar,
Mohanlal Sukhadia University,
Udaipur.

Dr. Santhosh Prabhu
Editor-in-Chief
Assistant Professor (Law),
SDM Law College, Centre for PG
Studies & Research in Law,
Mangalore
D.K. Karnataka, India





Dr Pallavi Singh
Editor-in-Chief
Assistant Professor (CUSB),
School of law and Governance,
Central University of South
Bihar, Gaya.



Advo. Tarun Agarwal
Editor-in-Chief
Lawyer in London and Mumbai
Registered Foreign Lawyer in
England and Wales



Aakansha Verma
Senior Editor
Assistant Professor,
Presidency school of Law,
Presidency University,
Bengaluru, Karnataka.

Shivani Gupta
Senior Editor
Assistant Professor,
KGP PG College,
Moradabad.



Students Editors

- 1. Advo. Anushree Tiwari**
- 2. Ashutosh Debata**
- 3. Akriti Sonwani**
- 4. Jatin Rana**
- 5. Sumit kumar**
- 6. Lalith Swetha**

Legalonus

Publisher
LegalOnus Publishing Team

LegalOnus Law Journal (LLJ)

INDEX

S. NO.	TOPIC	AUTHOR	PAGE NO.
1.	DYING DECLARATIONS IN INDIAN EVIDENCE ACT: LEGAL ANALYSIS AND CASE STUDIES	KAMNA KATIYAR	2-12
2.	PROXIMATE AND TENDENCY TESTS: KEY LEGAL TOOLS IN FREE SPEECH CASES	AHMAD USMAN	13-20
2.	CYBER LAW IN INDIA: THE SENTINEL OF THE DIGITAL FRONTIER	SATYA VRAT PANDEY	21-30
3.	ROLE OF TRADEMARK: MARKET DISTINCTIVENESS AND ANTITRUST IMPLICATIONS OF BRANDING	MITALI GUPTA & MEGHALI SWARNKAR	31-63
4.	RECENT TRENDS IN CYBERCRIME AND DATA PROTECTION LAW	AMAN KUMAR CHOUDHARY, SHAMSH S. AHSAN & SWEETY KUMARI	64-95
5.	CYBER FRAUDS AND THE LEGAL RESPONSE: A COMPARATIVE ANALYSIS OF INDIA, THE US, AND THE EU	AGAM SHARMA	96-117

LegalOnus Law Journal (LLJ)



***Dying declarations in Indian evidence act: legal analysis and
case studies***

By Kamna Katiyar

Legalonus

LegalOnus Law Journal (LLJ)

In the hon’ble supreme court of India

Naeem vs state of Uttar Pradesh

Petitioner-Naeem & another

Vs

Respondent-state of Uttar Pradesh & another

- Citation- 1978 of 2022
- Date of judgement- 5th march 2024
- Hon’ble judges- hon’ble justice B.R.gavai and hon’ble justice Sandeep Mehta

Introduction

The law of evidence elaborates on the principle which governs the law is that evidence which cannot be tested is not admissible in the court of law. In other words, the administration of oath and cross examination of the maker of a statement establishes the veracity of the same. Thus, hearsay evidence is no evidence.

Nevertheless, in situations, the law makes an exception as a matter of necessity such as where a man is on his deathbed and makes a statement relevant to the cause of death. The law attaches great solemnity and sanctity to the words of the dying man on the ground that at the verge of his likely departure from the earthly world, he will not indulge in falsehood and secondly, the exclusion of such evidence may result in miscarriage of justice in as much as the victim may be the only eye witness of a serious crime.

Dying declarations have solely relied upon for the purposes of conviction. However, over the years, dying declaration & Indian evidence act section 32 of the Indian evidence act 1872 speaks of

LegalOnus Law Journal (LLJ)

special statements. It comes into play only in specific situations, that is, when either the person is dead or not found or incapable of giving evidence or attendance cannot be procured without unreasonable delay. On proof of the former, the knowledge of the person who is unavailable should be transmitted to the court through some other person. Subsection (1) of the section enumerates that statements made by a person as to the cause and circumstances leading to his death are relevant and admissible in evidence as dying declarations.

The legal maxim "nemo moriturus praesumitur mentire"—"a man will not meet his maker with a lie in his mouth"—indicates the basis upon which dying utterances are allowed in evidence. These are extreme statements made when a person is near death, when all hope for the future has been lost, when all motivations for lying have been silenced, and when the mind has been moved to speak the truth by the strongest factors; a state so solemn and calm that the law feels compelled to acknowledge the statement's veracity.

In this case the supreme court focused heavily on the legal principle surrounding the admissibility and reliability of a dying declaration as the sole basis for conviction.

The court reaffirmed that a dying declaration holds significant evidentiary value in Indian law, especially when it is determined to be true, voluntary, and coherent. Consistent with past rulings, including *atbir v. Government of NCT of Delhi*, the court stated that a trustworthy dying declaration can independently support a conviction without the need for additional corroborative evidence. The rationale is that a person on the brink of death is unlikely to fabricate statements, making their declaration highly credible if verified by the court as genuine and unprompted.

Facts

- The complaint filed by Shahin Parveen (deceased), who was admitted to the district hospital in Moradabad at 02:20 pm on December 1, 2016, with 80% deep thermal and facial burns, was transcribed and sent to the police station katghar, district Moradabad, at 8:15 p.m. On December 1.

LegalOnus Law Journal (LLJ)

- In her lawsuit, the deceased claimed that the accused/appellants had burned her alive because they were forcing her into becoming a prostitute and engaging in illegal trafficking. A first information complaint was filed at police station katghar, district Moradabad, for the offence punishable under section 307 of the Indian penal code, 1860, based on the written complaint.
- She had been living in her married home with her two children, her brother-in-law (devar), pappi mashkooor (accused no. 1), and his wife Naeema (accused no. 2) for two years before the incident, following the death of the deceased's husband. The brother of Naeema is Naeem (accused no. 3).
- The accused/appellants allegedly began pressing the deceased into pursuing a career in prostitution and illegal trafficking after the death of her husband. The deceased was physically and sexually abused and ordered to leave the house because she refused to accept the same.
- The accused grabbed the dead and doused her with kerosene at around 1:30 pm on the day of the crime. The matchstick was lit by pappi mashkooor (accused no. 1) and hurled at her by Naeema (accused no. 2).
- The accused/appellants then surrounded her, making it impossible for her to flee. When the house caught fire, the deceased fled, and her neighbours extinguished the flames. They then notified her mother and brother, Islam Babli, who transported her to the hospital.
- At 8:15 p.m. On December 1, 2016, the firm was filed based on this written report and the deceased's thumb impression. After that, between 08:48 and 09:15 that same day, the deceased's final declaration was recorded. In it, she claimed that she and pappi mashkooor (accused no. 1) were still at odds over how to divide their joint home.

LegalOnus Law Journal (LLJ)

- The deceased and the accused/appellants got into another argument on the day of the occurrence at around 12:30 pm, during which accused no. 1 doused the dead with kerosene and lit her on fire. Naeem, his brother (accused no. 3), and his wife Naeema (accused no. 2) accompanied and helped him. After being brought to the district hospital in Moradabad by her brother Islam Babli, she was later transferred to Safdarjung hospital in new Delhi, where she ultimately passed away from her wounds.

Issues

- Whether Shahin Parveen's deathbed statement could be the only reason for the accused's conviction, especially considering the seriousness of the murder charge.
- Whether Shahin was in a state of mind that allowed him to make a trustworthy statement.
- If the court evaluates supporting evidence?

Argument of petitioner

- The petitioners argued that the dying declaration, made by the deceased, Shahin Parveen, was unreliable and could not be used exclusively to convict them. They pointed out inconsistencies in the timing of events, particularly that Shahin had been discharged from a district hospital in Moradabad and transferred to Safdarjung hospital in new Delhi, suggesting that her physical and mental state at the time of the declaration might have impaired her coherence.
- The defence argued that Shahin's severe burn injuries likely affected her ability to make a clear, voluntary statement. They contested that her critical condition would have

LegalOnus Law Journal (LLJ)

compromised her mental clarity, questioning whether she was truly fit to make such an important declaration.

- The petitioners, especially Naeema and Naeem, argued that Shahin's declaration did not specify their precise roles in the incident. While papa (mashkooor) was directly accused of setting Shahin on fire, Naeema and Naeem were only generally mentioned as "assisting" him, without specific actions attributed to them. The defence argued that such vague mentions did not meet the legal threshold for a murder conviction.
- The defence also raised procedural issues, questioning the chain of events and whether due process was observed in recording the declaration. They highlighted inconsistencies in the medical officer's certification of Shahin's mental and physical fitness, suggesting potential lapses that could invalidate the declaration as a basis for conviction.

Argument of respondent

- The state argued that the dying declaration was both credible and admissible as primary evidence, highlighting that Shahin Parveen, the victim, had provided a clear, voluntary, and coherent account identifying her attackers. The prosecution argued that, under Indian law, a dying declaration can serve as the sole basis for conviction if it inspires confidence in the court.
- To counter the defence's claims about Shahin's mental state, the state presented evidence from rd. A.k. Singh, the emergency medical officer, who certified that Shahin was in a fit mental and physical state to give a statement. The state argued that this medical certification validated the dying declaration's reliability, underscoring that Shahin was fully aware and conscious when making her declaration.

LegalOnus Law Journal (LLJ)

- The state cited established legal precedents where courts have upheld convictions based solely on dying declarations, if they are free from tutoring, coercion, or fabrication. The state argued that Shahin's declaration was in line with these precedents and should be considered sufficient to uphold the conviction.
- The prosecution highlighted that the defence did not produce any substantial evidence to challenge the declaration or contradict Shahin's account. With no eyewitnesses or material evidence opposing the declaration, the state asserted that there was no basis to doubt its credibility.

Court's reasoning

- The court emphasised that, because of the circumstances surrounding their making, dying declarations are presumed to be true. This approach has been upheld in earlier decisions such as *Khushal Rao v. State of Bombay* (1958)¹. In identifying papi as the culprit, the court determined that Shahin's statement was clear and consistent, which supported the use of her declaration as reliable evidence.
- The accompanying medical officer's certification, which the court cited, was essential in confirming the accuracy of her dying declaration. The court cited the 2002 decision in *Laxman v. State of Maharashtra*,² which held that for a declarant's statement to be accepted, their mental health had to be verified.
- The responsibilities that Shahin's declaration assigned to each accused were closely scrutinised by the court. Although papi was unmistakably implicated as the person who lit her on fire, it decided that the allusions to Naeema and Naeem were ambiguous and lacked precise acts. The court decided that for a conviction to be supported, a dying declaration must explicitly outline each accused person's involvement, citing the precedent established

¹ AIR 1958 SC 22

² AIR 2002 SC 2973

LegalOnus Law Journal (LLJ)

in *panchhi v. State of up.* (1998)³. As a result, Naeema and Naeem were acquitted because of this lack of detail.

- The court restated that, provided it satisfies the requirements of specificity, voluntariness, and dependability, a dying declaration may be the only foundation for conviction. This position complies with earlier decisions, such as *atbir v. Government of NCT of Delhi* (2010)⁴, which determined that the statement's credibility is further increased by the lack of influence or pressure.
- The court concluded that Shahin's voluntary and cogent declaration adequately complied with these legal requirements.

Judgement

According to the court's unequivocal ruling, a dying declaration may serve as the only foundation for a conviction provided it engenders the court's complete trust. The court must be convinced that the dead were in a sound mental state when they made the statement and that it was not the product of coercion, imagination, or tutoring. Furthermore, it has been decided that the court might establish its conviction without any additional confirmation if it is confident that the dying declaration is accurate and voluntary.

Furthermore, it has been decided that there cannot be a legislation that states that a deathbed declaration cannot serve as the only foundation for conviction unless it is supported by evidence. It has been decided that the requirement for corroboration is just a precautionary regulation. According to the court, there will be no legal barrier to using it as the basis for conviction even in the absence of corroboration if, after careful examination, the court is convinced that it is true, free from attempts to persuade the deceased to make a false statement, and coherent and consistent.

³ 1998) 7 SCC 177

⁴ 2010) 9 SCC 1

LegalOnus Law Journal (LLJ)

The court carefully analysed the evidentiary value of the declaration and assessed the specific roles attributed to each accused in the statement:

- The supreme court concluded that Shahin's clear and direct accusation against papi, coupled with her mental fitness at the time of the statement (certified by medical personnel), satisfied the legal standards for a conviction based solely on a dying declaration. The court sentenced him to life imprisonment under section 302 (murder) of the Indian penal code.
- For Naeema and Naeem, the court found that Shahin's declaration did not specify their actions with sufficient clarity. While Shahin mentioned that they "assisted" papi, the court held that this general reference was insufficient to establish their direct involvement in the crime beyond a reasonable doubt. Consequently, the supreme court acquitted both Naeema and Naeem, emphasising that a dying declaration, even if reliable, must provide clear details regarding the specific roles of each accused if it is to be the sole basis for conviction.
- The court reaffirmed the legal principle that a dying declaration can be used as the sole basis for conviction if it is consistent, voluntary, and given in a sound mental state. However, the court underscored that each accused's role must be explicitly described, especially in cases involving multiple individuals, for the declaration to justify a conviction without additional corroborative evidence.

Case analysis

The supreme court's ruling upholds the idea that, although though deathbed declarations can be effective means of obtaining convictions, their usage needs to be closely examined, particularly when there are several defendants. The significance of precision in deathbed pronouncements is highlighted by the supreme court's ruling to acquit Naeema and Naeem. This supports the idea that, even while emotional impact might influence a statement's impact, legal norms demand that acts be clearly attributed to support a conviction.

LegalOnus Law Journal (LLJ)

The supreme court upholds the stability of legal principles pertaining to dying statements by drawing on well-established cases. The court supported its ruling by referencing earlier decisions, which also served as a model for instances with related difficulties in the future. Thus, the case is a prime example of the fine line the courts must draw between providing victims with justice and guaranteeing the accused receives fair treatment. As a precaution against unjust conviction, Naeema and Naeem's acquittal highlights the need for the legal system to uphold the rights of all parties. In situations where emotive narratives may result in rash decisions, this part of the decision is essential to preserving public confidence in the judicial system.

Conclusion

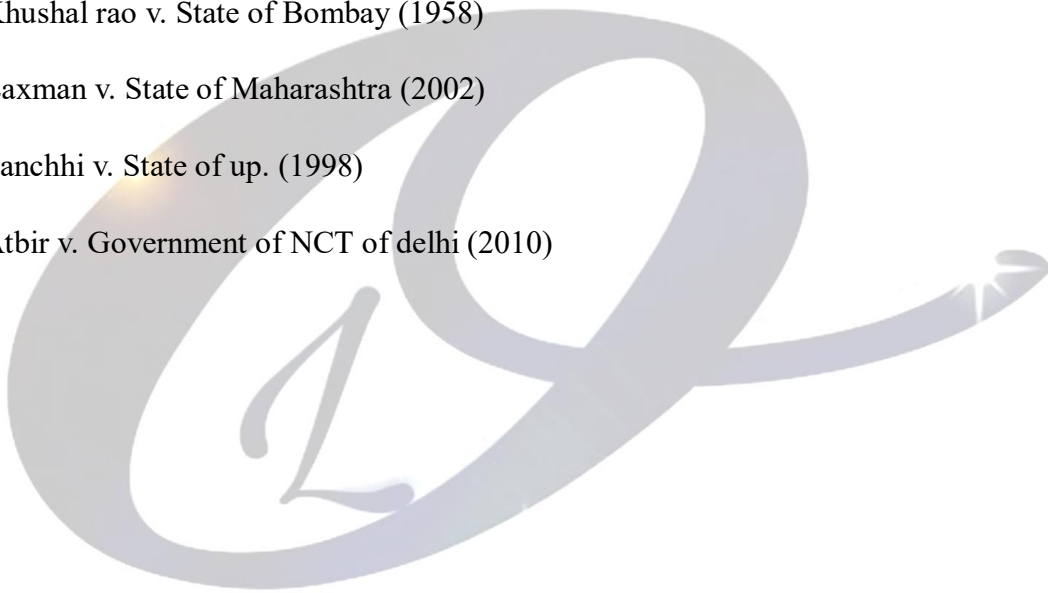
This case exemplifies the intricate relationship between the principles of justice and the evidentiary standards applied in criminal law, particularly regarding dying declarations. The supreme court's judgement reinforced the validity of such declarations as critical evidence, provided they are made voluntarily and with mental clarity also emphasised the necessity for specificity when multiple defendants are involved, as seen in the acquittal of Naeema and Naeem due to the lack of clear attribution of actions. This decision not only highlights the importance of protecting the rights of the accused but also underscores the legal system's commitment to ensuring fair trials.

The dying declaration is a significant piece of evidence. It may be the last and most pertinent available evidence concerning the commission of a crime. Accordingly, the law of evidence makes it relevant as well as admissible. It is also substantive evidence against the accused and a conviction can be based solely on a dying declaration. Given the importance attached to dying declaration, the courts have evolved various principles to guide it. It should strike to be genuine, free from all doubts, stating the true story of the maker. In case the court entertains any doubt about the same, it is imperative for the court to investigate corroborative evidence to test the truthfulness of the dying declaration. It is the duty of the court to consider the dying declaration in its correct perspective and satisfy itself of its truthfulness before it can proceed to convict an accused. This case serves as a vital reference point for future adjudications involving dying declarations, illustrating the need for scrutiny and adherence to established legal standards.

LegalOnus Law Journal (LLJ)

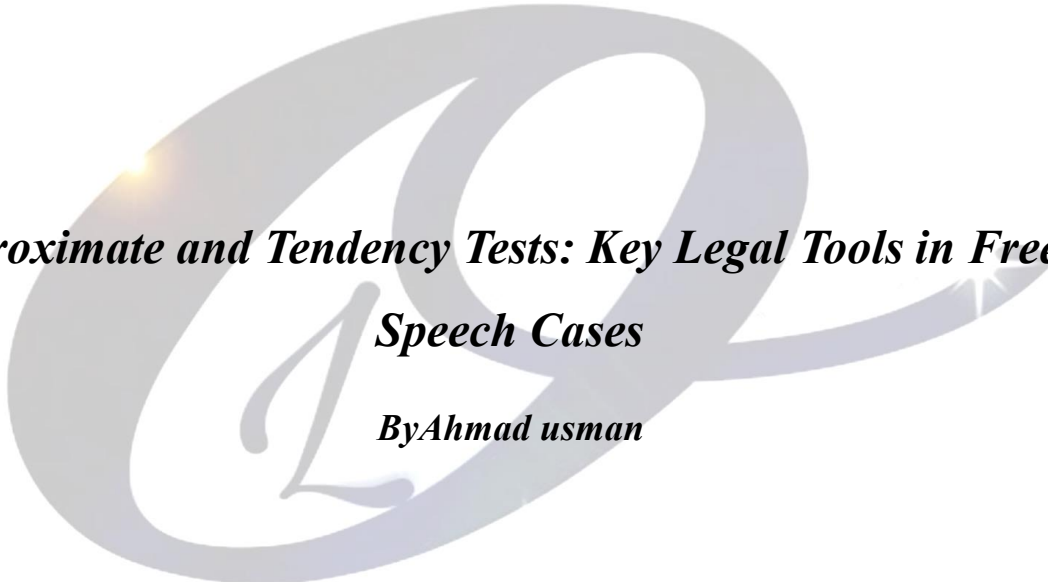
References

- Ratanlal & dhirajlal law of crimes
- V. R. Manohar and w. R. Manohar's law of evidence
- "Law of dying declaration: a legal analysis" - article by Shailendra Kumar
- "Justice and judicial interpretation in Indian courts" - journal article in Indian law review
- "principles of criminal law" by k.d. Gaur
- Khushal rao v. State of Bombay (1958)
- Laxman v. State of Maharashtra (2002)
- Panchhi v. State of up. (1998)
- Atbir v. Government of NCT of delhi (2010)



Legalonus

LegalOnus Law Journal (LLJ)



***Proximate and Tendency Tests: Key Legal Tools in Free
Speech Cases***

By Ahmad usman

Legalonus

LegalOnus Law Journal (LLJ)

Abstract:

This paper explores the legal standards of the proximate and tendency tests used by Indian courts to balance free speech and public order. In democratic societies like India, freedom of speech, as enshrined under article 19(1)(a) of the constitution, is a fundamental right. However, article 19(2) permits the state to impose reasonable restrictions on this right, including for public order concerns. The judiciary employs both the proximate and tendency tests to evaluate whether speech poses a sufficient threat to justify restrictions. While both tests aim to maintain public peace, they differ significantly in their criteria and implications.

The proximate test requires a close and immediate connection between speech and the risk of public disorder, adhering to a "clear and present danger" standard. Based on the jurisprudential roots of Justice Holmes's famous doctrine from *Schenck v. United States* (1919), this test has been favoured by the Indian judiciary. It demands evidence of an imminent threat, preventing restrictions based on hypothetical or distant dangers. This approach was upheld in landmark cases such as *Superintendent, Central Prison, father v. Ram Manohar Lohia* (1960), where the Supreme Court emphasised that only speech that directly incites immediate disorder should be restricted. More recently, the *Shreya Singhal v. Union of India* (2015) judgment reiterated the proximate test's role in protecting free expression, especially in the digital age.

In contrast, the tendency test allows for speech restrictions based on the potential or tendency of the expression to disrupt public order, without requiring an immediate or direct connection. This standard stems from the "bad tendency" doctrine, a broader approach granting the government preventive powers to restrict speech that may incite gradual social unrest. Historically, the tendency test was applied in colonial India to curtail dissenting voices under laws such as the Indian Press Act of 1910. In *Kedar Nath Singh v. State of Bihar* (1962), the Supreme Court upheld section 124a of the IPC (sedition), indicating that speech with a tendency to incite violence could be curtailed under this test. However, the judiciary has generally avoided the tendency test in recent rulings, given its potential to lead to arbitrary restrictions and undue government control over speech.

LegalOnus Law Journal (LLJ)

Through a comparative analysis, this paper underscores the distinct features of the two tests. The proximate test, with its high threshold for restriction, safeguards democratic values by limiting state intervention. The tendency test, while useful for preventive action, presents risks of overreach, potentially stifling free expression. The paper discusses these tests' applications in the Indian legal landscape, noting the judiciary's preference for the proximate test to uphold constitutional freedoms.

In conclusion, while both tests are vital tools in the interplay between free speech and public order, the proximate test aligns more closely with democratic ideals. Nonetheless, with the rapid evolution of digital communication, courts may need to consider new approaches to maintain this delicate balance in the future. This paper highlights the importance of adapting these principles to contemporary challenges without compromising individual rights.

Keywords: proximate test, tendency test, public order, freedom of speech.

Introduction:

The right to freedom of speech is a cornerstone of democratic societies, enabling individuals to express ideas, debate, and engage in civic discourse. However, this freedom is not without limits, especially when public order is at risk. In India, as in many democracies, the courts have crafted legal standards to determine when restrictions on speech are justified to prevent disruptions. Two prominent standards, the proximate test and the tendency test, serve as essential tools in this analysis.

While both tests examine the link between speech and the potential for disorder, they differ significantly in their scope and application. The proximate test requires an immediate, direct connection to public disorder, whereas the tendency test looks for a broader, more generalized risk. This article explores the origins, applications, and consequences of these tests in India, emphasizing their implications on the balance between free expression and public order.

Free speech and public order in the Indian context

LegalOnus Law Journal (LLJ)

In India, article 19(1)(a) of the constitution guarantees the right to free speech, allowing citizens to communicate their ideas freely. However, article 19(2) allows the state to impose reasonable restrictions on this right for the sake of public order, among other concerns. The Indian judiciary has consistently emphasized that these restrictions must be carefully calibrated to protect public order without infringing unnecessarily on free speech.

This is where the proximate and tendency tests come into play. By providing distinct legal frameworks, these tests allow the courts to evaluate whether restrictions on speech are necessary and proportionate, aiming to uphold democratic values while maintaining societal peace.

The proximate test: a high threshold for restricting speech

The proximate test is a standard that limits speech restrictions to cases where a direct and immediate threat to public order is present. In other words, under the proximate test, speech can only be curtailed if it has a clear, strong probability of inciting immediate public disorder.

- **Origins of the proximate test**

The proximate test is based on the principle of "clear and present danger," a concept that emerged from Justice Oliver Wendell Holmes Jr. in the U.S. case *Schenck v. United States* (1919). Holmes argued that speech could be restricted only if it poses a "clear and present danger" of causing harm that the government has a right to prevent.

This principle resonated in Indian jurisprudence, as the Indian judiciary sought to protect free speech while allowing the government to curb speech that posed a real threat to public order. The proximate test thus reflects a commitment to limiting restrictions on speech to cases where there is a high likelihood of immediate harm.

- **Proximate test in Indian jurisprudence**

The Supreme Court of India has often applied the proximate test when interpreting restrictions on free speech, particularly in cases involving public order. A landmark case, *Superintendent, Central Prison, Fatehgarh v. Ram Manohar Lohia* (1960), set an important precedent by emphasizing the

LegalOnus Law Journal (LLJ)

need for a close, proximate link between speech and public disorder. The court held that restrictions must be connected to a serious and immediate threat, reinforcing that vague or hypothetical threats are not sufficient grounds for curbing free speech.

In more recent cases, such as *Shreya Singhal v. Union of India* (2015), the supreme court struck down section 66a of the information technology act, citing the importance of clarity and specificity in speech restrictions. The court underscored that restrictions should only apply to speech that incites imminent violence or disorder, upholding the proximate test as a necessary standard for safeguarding free speech.

- **Advantages and challenges of the proximate test**

The proximate test has significant advantages for freedom of speech, as it sets a high bar for state intervention. By requiring a direct and immediate threat, the test minimizes the risk of unnecessary restrictions, preserving individuals' rights to express dissent or unpopular opinions.

However, the proximate test's strict requirements can also limit the government's ability to act preventively. In cases where speech incites cumulative harm or slower-burning social disruptions, the proximate test may make it difficult to restrict speech in time to prevent escalation.

The tendency test: a broader approach to preventive action

In contrast to the proximate test, the tendency test allows the restriction of speech if it merely tends to disrupt public order. Under this test, authorities can impose restrictions based on the potential or likelihood of harm, without requiring a direct or immediate threat.

- **Origins and legal foundations of the tendency test**

The tendency test traces its roots to the "bad tendency" doctrine, which permits restrictions on speech that could, in some way, lead to public disorder. Historically, this test has been applied to curb speech that authorities believe has the potential to incite social unrest or disrupt peace.

LegalOnus Law Journal (LLJ)

In colonial India, the tendency test allowed broad state control over publications and speeches. For example, the Indian Press Act of 1910 imposed restrictions on publications with "bad tendencies" to suppress critical voices against British rule. This approach to regulation favoured preventive action over the protection of free speech.

- **Application of the tendency test in Indian law**

Indian courts have occasionally used the tendency test in cases involving speech that has the potential to incite violence or public disorder, even if the threat is not immediate. One notable case, *Kedar Nath Singh v. State of Bihar* (1962), addressed the constitutionality of section 124a of the Indian Penal Code (sedition). The Supreme Court upheld the section, noting that speech that "tends" to incite violence or disrupt public order can be restricted, thereby applying a form of the tendency test.

However, the judiciary has largely moved away from this approach in favor of more stringent standards, as seen in cases like *S. Rangarajan v. P. Jagjivan Ram* (1989). In this case, the court rejected the tendency test, emphasizing the importance of a direct and immediate connection to public disorder. This decision reflected the judiciary's preference for narrower restrictions on speech, highlighting the potential for the tendency test to infringe upon fundamental rights.

- **Strengths and limitations of the tendency test**

The tendency test is advantageous for authorities who seek to prevent unrest, as it allows for restrictions based on general potential rather than specific threats. This approach is useful in cases where speech may gradually lead to disorder, such as inflammatory rhetoric or propaganda.

However, the tendency test is highly susceptible to overreach. By focusing on vague risks, it grants the government considerable discretion, potentially leading to arbitrary or unjustified restrictions on speech. This can undermine democratic principles, as it allows the government to limit dissent or unpopular opinions based on hypothetical threats rather than concrete risks.

Comparing the proximate and tendency tests

LegalOnus Law Journal (LLJ)

The proximate and tendency tests represent two distinct approaches to balancing free speech and public order. Below is a comparative analysis of their key aspects:

<u>Aspect</u>	<u>Proximate test</u>	<u>Tendency test</u>
Focus	Direct, immediate threat to public order	General tendency to disrupt public order
Threshold	High – requires clear and present danger	Low – based on potential risk
Implications	Protects free speech with strict criteria	Allows preventive action but risks overbroad limits
Risk of abuse	Low, as it requires clear proof of imminent harm	High, as it can lead to vague or arbitrary restrictions

The proximate test: a preferred standard for the Indian judiciary

The Indian judiciary has generally favoured the proximate test, emphasizing that speech restrictions should be narrow and linked to an immediate threat. This preference is grounded in democratic principles, which prioritize individual rights and restrict state interference unless necessary.

In the landmark *Shreya Singhal v. Union of India* case, the Supreme Court articulated that "mere discussion or advocacy, no matter how unpopular, should not be restricted unless it incites imminent violence." This judgment underscored the proximate test's importance in protecting free speech while upholding the need for public order.

Challenges and future directions

Despite its clear benefits, the proximate test presents challenges. In an age of digital communication, where harmful content can spread rapidly and subtly incite unrest, the need for

LegalOnus Law Journal (LLJ)

preventive measures has increased. Social media and online platforms can quickly amplify speech that might initially appear innocuous but could lead to cumulative harm.

Some legal experts argue that the proximate test may require adjustments to address these modern challenges, allowing for a more nuanced approach to online speech. However, any shift towards a broader interpretation must be carefully managed to prevent overreach.

Conclusion

The proximate and tendency tests play a crucial role in balancing free speech and public order, offering distinct frameworks for assessing the risk of speech-related disruptions. The proximate test aligns closely with democratic principles, demanding clear, immediate threats before speech can be restricted. The tendency test, while useful for preventive action, carries risks of arbitrary or excessive state control.

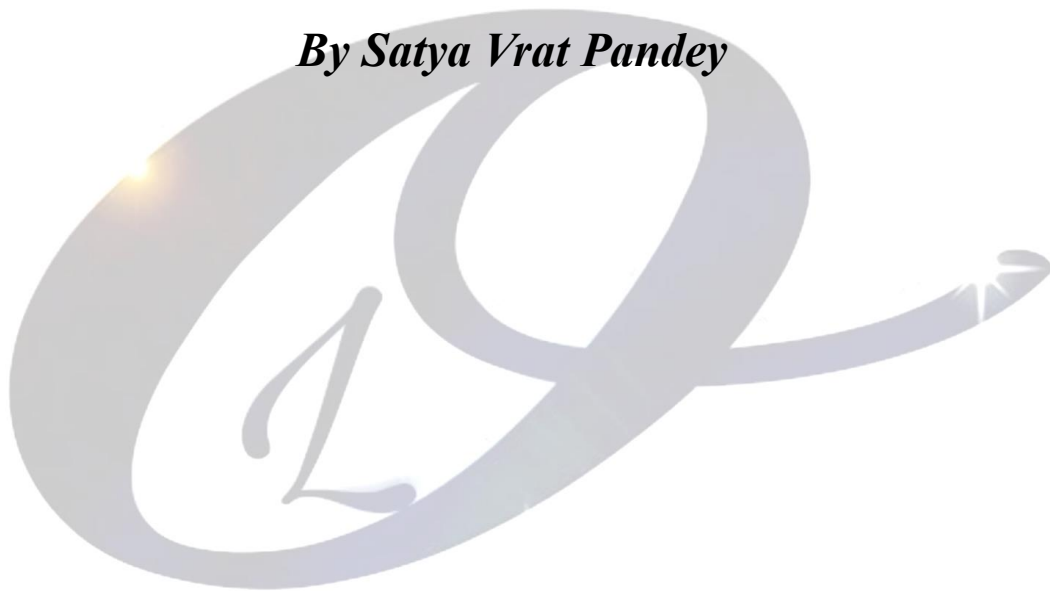
In india, the judiciary's preference for the proximate test reflects a commitment to safeguarding free speech while maintaining public order. Moving forward, the challenge lies in adapting these principles to address the complexities of modern communication without compromising fundamental rights

Legalonus

LegalOnus Law Journal (LLJ)

Cyber law in India: the sentinel of the digital frontier

By Satya Vrat Pandey



Legalonus

LegalOnus Law Journal (LLJ)

Abstract

The rapid proliferation of technology and the internet in the contemporary digital age has highly changed the way individuals and organisations interact, share ideas, and conduct commerce. As one of the largest online markets globally, india has seen a corresponding rise in cyber activity, which poses both opportunities and challenges. The need for a robust legal framework to regulate the digital landscape has never been more pressing. Cyber law in india evolves as a crucial protector of the digital realm, addressing issues related to online privacy, data protection, and criminality. The information technology act of 2000 serves as the foundation of cyber law in india, providing the legal framework to combat cyber offences and establishing a platform for electronic commerce. This legislation has evolved over the years via several changes, particularly the information technology (amendment) act of 2008, which expanded legal protections to include provisions for data privacy, cyberterrorism, and enhanced penalties for cybercrimes. Despite these legal advancements, the implementation of cyber law in india encounters numerous challenges, including rapid technological progress that surpasses existing legislation, a significant deficiency in public awareness concerning cyber rights and responsibilities, and insufficient infrastructure and resources for law enforcement agencies tasked with enforcing these laws. The jurisdictional complexity arising from the global nature of the internet hinders international cyber law enforcement. The Indian government must adopt a proactive approach, focussing on continuous legislative updates, public education initiatives, and enhancements in law enforcement capabilities to effectively address these challenges. India can establish a more secure digital landscape by fostering collaboration among many stakeholders, including the government, law enforcement, and the public, therefore ensuring that the benefits of technological advancement are harnessed while mitigating the risks associated with cyber assaults. Understanding and implementing cyber legislation will safeguard personal freedoms and contribute to the security and reliability of the evolving digital economy.

Keyword: cyber law, privacy laws, intellectual property rights, cybersecurity policy, online defamation, digital security.

LegalOnus Law Journal (LLJ)

Introduction

The information technology act, 2000 (it act) is India's primary law governing cyber activities, enacted to provide legal recognition to electronic transactions and curb cybercrimes. It was introduced in response to the increasing use of digital platforms for commerce and communication, aligning india with global standards like the united nations' model law on electronic commerce. The act addresses several key areas:

1. Electronic contracts: it grants legal validity to e-contracts, enabling businesses to function efficiently in the digital space.
2. Digital signatures: by legitimizing digital signatures, it ensures secure authentication of electronic records.
3. Cybercrime regulation: the act defines and penalizes crimes like hacking, identity theft, data breaches, and cyberstalking.
4. E-governance: it facilitates government services online, making governance more accessible and transparent.

Significantly, the it acts establishes the certifying authorities (case) and the cyber appellate tribunal for resolving disputes and promoting trust in digital interactions. India's digital revolution in the last two decades has transformed communication and significantly modified how individuals and businesses interact and execute transactions. The digital realm has seamlessly integrated into everyday life and has become an essential element of both personal and professional interactions due to the proliferation of the internet and mobile technology. The efficiency and convenience of digital platforms, including e-commerce, online banking, social networking, and telecommuting, have facilitated economic expansion and enhanced connectivity for millions of individuals. However, this rapid advancement has also given rise to several issues that pose significant threats to individuals and enterprises alike. In the contemporary digital landscape, issues such as cybercrime, data breaches, identity theft, and privacy violations have alarmingly grown prevalent. The risks associated with the use of increasingly personal and sensitive data transferred online

LegalOnus Law Journal (LLJ)

have intensified, prompting concerns over the integrity and security of online transactions. Considering these challenges, cyber law in india has gained significance as a mechanism to safeguard individuals and organisations from the many threats associated with the digital age. This regulatory framework aims to enhance the safe and secure use of digital technology while mitigating the risks associated with cyber operations. O address the challenges posed by the digital age, india requires a multi-pronged approach that combines legislative measures, technological advancements, and awareness initiatives. To combat cybercrime, there is a need for advanced threat detection tools powered by ai, strengthened cyber policing units, and amendments to the information technology act, 2000,⁵ to address emerging threats. For preventing data breaches, strong encryption protocols, a zero-trust security framework, and compliance with global data protection standards like GDPR are essential. Identity theft can be mitigated through multi-factor authentication (mfa), biometric verification, and real-time monitoring systems. To safeguard privacy, robust legislation such as India’s digital personal data protection act of 2023,⁶ should be enforced, along with privacy-by-design principles in technology and tools that allow users control over their data. Ensuring the integrity and security of online transactions requires the adoption of blockchain technology, mandatory end-to-end encryption in payment systems, and regular security audits. Broader initiatives include implementing a national cybersecurity strategy, fostering public-private partnerships for innovative solutions, training law enforcement and judicial bodies in cyber laws, and strengthening international cooperation to address cross-border cybercrimes. These measures collectively aim to create a safe, secure, and trustworthy digital environment for individuals and enterprises alike. Cyberlaw seeks to provide a secure digital environment by legislation governing online activities and transactions, hence fostering trust in technology and creativity. The need for robust cyber laws is paramount as india advances on its digital trajectory,

⁵ Information Technology Act, No. 21 of 2000, (India)

⁶ Digital Personal Data Protection Act, No. 13 of 2023, (India).

LegalOnus Law Journal (LLJ)

since they are essential for safeguarding the rights and interests of individuals and enterprises in an increasingly interconnected society.⁷

Historical context and evolution of cyber law in india

In the late 1990s, the Indian government saw the need to establish a legislative framework to regulate electronic transactions and tackle the increasing prevalence of cybercrime issues.⁸ This marked the start of the trajectory that cyber law will follow in India. The Information Technology Act of 2000 (IT Act) was enacted to affirm the legal validity of electronic transactions, provide a framework for data protection, and delineate charges related to cybercrime. The Information Technology Act was a pivotal moment that facilitated further advancements in cyberlaw. Since its creation, the Information Technology Act has seen many amendments to meet developing issues in the digital domain. The Information Technology (Amendment) Act of 2008⁹ notably broadened existing legislation by including measures for data security and cyberterrorism while also augmenting punishments for cyber offences. The formation of the Cyber Appellate Tribunal further offered a forum for resolving disputes and appeals related to breaches of cyber law.

Key provisions of cyber law in india

The Information Technology (IT) Act encompasses several critical provisions addressing key aspects of cyber law. It provides legal recognition to electronic records and digital signatures, enabling secure online transactions and communication. The act also emphasizes data protection and privacy, mandating guidelines for the collection, storage, and processing of personal information, while requiring organizations to adopt reasonable security practices to safeguard sensitive data. Additionally, it categorizes various cyber offences, such as hacking, identity theft, phishing, and cyberstalking, prescribing penalties to deter cybercrimes and offering victims legal recourse. The

⁷ Simplilearn, *What is Cyber Law?*, Simplilearn (July 11, 2023), <https://www.simplilearn.com/what-is-cyber-law-article>.

⁸ InfoSec Awareness, *Cyber Laws of India*, InfoSec Awareness (last visited Nov. 14, 2024), <https://infosecawareness.in/cyber-laws-of-india>.

⁹ Information Technology (Amendment) Act, No. 10 of 2009, India Code (2009).

LegalOnus Law Journal (LLJ)

act outlines the role and responsibilities of intermediaries, like social media platforms and online service providers, granting them safe harbour protection from liability for third-party content, provided they exercise due diligence. It also addresses the regulation of online content, including issues like hate speech, obscenity, and defamation, empowering law enforcement agencies to act against violations. However, the act faces limitations in addressing challenges posed by emerging technologies like blockchain and artificial intelligence (ai). These rapidly evolving technologies introduce complexities in areas such as decentralized governance, data ownership, and algorithmic accountability, which the act does not adequately cover. This gap underscores the need for updating the legal framework to ensure its relevance and effectiveness in the face of technological advancements.

Challenges in the implementation of cyber law

Despite the robust framework established by the information technology act, 2000 (it act), india faces significant hurdles in the implementation of its cyber laws. The rapid pace of technological innovation, coupled with issues such as a lack of awareness, inadequate resources, and jurisdictional complexities, undermines the efficacy of these regulations.

1. Challenges due to rapid technological evolution

Cybercriminals continually develop sophisticated methods such as ransomware attacks and advanced persistent threats (apts),¹⁰ often outpacing legislative updates. For instance, the wannacry ransomware attack (2017),¹¹ which affected over 150 countries, including india, revealed gaps in India's preparedness to tackle widespread cyber incidents. Despite the its act's provisions, many affected Indian institutions lacked the tools and expertise to effectively respond.

¹⁰ Imperva, *APT (Advanced Persistent Threat)*, Imperva, <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/> (last visited Nov. 14, 2024).

¹¹ Cloudflare, *WannaCry Ransomware*, Cloudflare, <https://www.cloudflare.com/en-gb/learning/security/ransomware/wannacry-ransomware/> (last visited Nov. 14, 2024).

LegalOnus Law Journal (LLJ)

2. Awareness gaps among stakeholders

A lack of awareness about digital rights and cyber laws leaves individuals and organisations vulnerable. For example, during the Aadhaar data breach incidents, millions of Indians were exposed to potential misuse of their sensitive data. Many victims were unaware of their rights under laws such as the IT Act or how to seek redress.

3. Inadequate infrastructure and expertise

Law enforcement agencies often lack the technical expertise necessary to investigate and prosecute cybercrimes. The ATM hacking case of 2018, where Indian banks suffered significant losses due to malware attacks on ATMs, highlighted this limitation. Investigations revealed that outdated security systems and insufficient cyber forensics expertise in local enforcement hindered timely resolution.

4. Cross-border jurisdiction issues

The global nature of the internet complicates enforcement. Cybercrimes often involve actors and servers located in different jurisdictions, making it difficult to determine the applicable law.

- Case study of the Sony pictures hack (2014)¹²:- though not directly involving india, this case demonstrates the difficulty in attributing cyberattacks across borders. The hack, allegedly conducted by north Korean actors, exploited vulnerabilities across various nations' infrastructure. For Indian law enforcement, similar attribution issues arose during incidents like the cosmos bank cyber heist (2018), where hackers allegedly from Pakistan and other nations siphoned ₹94 crore using malware and cloned cards. Cooperation with international agencies became critical, but jurisdictional ambiguities delayed the process.

¹² Coverlink, *Sony Pictures Entertainment Hack*, Coverlink, <https://coverlink.com/case-study/sony-pictures-entertainment-hack/#:~:text=From%20there%2C%20the%20film's%20distribution,an%20advanced%20form%20of%20malware> (last visited Nov. 14, 2024).

LegalOnus Law Journal (LLJ)

- Case study of the silk road investigation¹³:- while this case primarily unfolded in the u.s., its lessons are pertinent for india. The investigation into the illegal online marketplace silk road relied on international collaboration. For india, enforcing laws against illicit activities on the dark web faces similar jurisdictional hurdles. Investigations into cases involving illegal drug trade or counterfeit currency on the dark web have often hit roadblocks due to non-cooperation from entities based in foreign jurisdictions.

5. Data localization and conflicting laws

India's increasing demand for data localisation, as outlined in the draft personal data protection bill, clashes with global norms. For example, social media companies operating in india have faced challenges balancing compliance with local laws and foreign regulations like the general data protection regulation (GDPR)¹⁴ in the European union.

The role of government and law enforcement

To address these difficulties, the government must proactively improve the framework of cyberlaw. Thus, this requires the ongoing enactment of legislative amendments to tackle growing dangers and technological progress, ensuring the legal system remains effective and relevant. The efficacy of public awareness initiatives relies on the education of the populace on cyber law, digital rights, and safe online practices. Information may be disseminated to a vast audience inside schools, universities, and community groups.¹⁵ law enforcement agencies must provide money and training to improve their ability to fight cybercrime. Through partnerships with information technology firms and cybersecurity experts, law enforcement agencies may get the resources and expertise

¹³ Crime and Justice, *Inside the Darknet Takedown of Silk Road*, Crime and Justice, <https://www.crimeandjustice.org.uk/publications/cjm/article/inside-darknet-takedown-silk-road> (last visited Nov. 14, 2024).

¹⁴ GDPR-Info, *General Data Protection Regulation (GDPR) Compliance Guidelines*, GDPR-Info, <https://gdpr-info.eu> (last visited Nov. 15, 2024).

¹⁵ UpGuard, *Cybersecurity Regulations in India*, UpGuard (last visited Nov. 14, 2024), <https://www.upguard.com/blog/cybersecurity-regulations-india>.

LegalOnus Law Journal (LLJ)

required to proficiently address cyber threats. The worldwide nature of cybercrime necessitates paramount coordination among international law enforcement authorities. The establishment of multinational alliances and treaties is advantageous for addressing cyber threats by promoting the flow of knowledge and resources.¹⁶

Conclusion

In conclusion, cyber law in india is a crucial protector of the digital realm, as it provides the necessary legal framework to address the intricacies of our linked online landscape. The advancement of technology is giving rise to new issues, underscoring the increasing need for cyber legislation. Legal systems must adapt concurrently with technological breakthroughs, including blockchain, artificial intelligence, and the internet of things (iot). This will facilitate the minimization of emerging hazards and the establishment of strong safeguards for all consumers. To advance toward a safe digital environment, collaboration and active engagement from individuals, corporations, and communities are essential. Strengthening public-private partnerships can foster the sharing of knowledge and resources, while establishing a national cybersecurity task force ensures coordinated responses to cyber threats. Promoting cybersecurity awareness campaigns and facilitating skill development in cybersecurity will empower individuals to protect themselves and navigate the digital realm effectively. Furthermore, incentivizing research and innovation in cybersecurity, particularly in ai-based threat detection and secure iot systems, can provide robust defences. Mandating cybersecurity standards for iot devices and enhancing international cooperation to establish unified cyber norms will also play pivotal roles. Governments must implement robust data protection laws aligned with global best practices to ensure accountability among corporations. Accessible reporting mechanisms and rapid response teams are critical to addressing incidents swiftly and minimising damage. Corporations should build a culture of transparency by disclosing cybersecurity breaches and working with regulators

¹⁶ World Economic Forum, *Partnership Against Cybercrime*, World Economic Forum (last visited Nov. 14, 2024), <https://www.weforum.org/projects/partnership-against-cybercrime/>.

LegalOnus Law Journal (LLJ)

to improve accountability while safeguarding sensitive data. The formulation of effective strategies to combat cybercrime relies on collaboration among government entities, technology firms, and law enforcement. A synergistic approach is essential to address existing risks and future challenges. By establishing a robust cyber legal framework, fostering trust, and creating a secure digital ecosystem through these measures, we can reconcile innovation with protection. The goal is to cultivate a flourishing digital environment where basic rights and freedoms harmoniously coexist with technological advancement. Together, we can ensure that the digital realm remains a domain of opportunity and security, benefiting individuals, enterprises, and society while promoting exceptional development and innovation.



Legalonus

LegalOnus Law Journal (LLJ)

***Role of trademark: market distinctiveness and antitrust
implications of branding***

By

Mitali Gupta

Meghali swarnkar

Legalonus

LegalOnus Law Journal (LLJ)

Abstract:

In today's world, intellectual property rights (ipr) play a crucial role in facilitating the trade and the economy of the nations which also ensures that intangible property like trademarks, inventions, and creative works should not be exploited by unauthorized users. Intellectual property provides that the ideas and the innovation, marks are not duplicated and must not be stolen by the unauthorized user; it leads to the uniqueness and the distinctiveness of the brand from the markets.

The trademark plays an important role and is part of the ip laws that protect intangible assets. However, earlier it was not so concerned but now demands of branding of your assets have received a lot of attention as intangible assets need to be protected so that innovations and inventions can be done without the fear of competitive interference. Here the trademarks rights provide the legal basis to protect the assets under the trademark laws.

Trademarks help brands distinguish their products and services in competitive markets, allowing customers to identify the source and quality of the original product. However, competition law regulates anti-competition practices, and trademarks can intersect with anti-trust concerns when monopolizing market segments.

This paper examines trademarks and how a simple branding change can balance market distinctiveness and competitive fairness. It also examines the nature of trademarks and their relationship to competition law and intellectual property rights. Finally, it analyzes how bonding strategies can result in antitrust implications and specifically create barriers to market access. It is said to be that ip laws cumulatively ensure competition among brands in the business world.

Keywords: trademark, brand loyalty, branding, antitrust concern in trademark, trademark rights.

1. Introduction: -

LegalOnus Law Journal (LLJ)

The term property had been derived from the Latin word proprietary which means the things the things which are owned. In ancient times, the word property only includes corporeal property nothing more than that. But now, the meaning of property gets wider. The properties can be of two types which are tangible and intangible i.e. Touchable and non-touchable. Examples of physical property that can be seen and felt include real estate, homes, jewelry, money, and further ahead. However, certain types of property are intangible. Among these is the right to intellectual property. In this case, r.c. Cooper v. Uoi¹⁷. The supreme court has correctly provided a comprehensive definition of property as it is the highest right, a man can have over anything, including the right to land, tenements, goods, or chattels that are not dependent on the courtesy of others. It includes ownership, estates, and interests in physical property, as well as rights like patents, trademarks, and copyrights, as well as rights in persona that can be transferred or transmitted, like debts. It also denotes a beneficial right to something thought to have monetary value, particularly about succession transfers and the potential for harm. Now, this form of property called intellectual property come into existence and it is growing.

The rights granted to people over their creative works, including inventions, literary and artistic productions, and names, symbols, and pictures used in trade, are known as intellectual property rights, or ipr. The "intellectual property" refers to how the human mind and intellect develop. Despite being hidden property, intellectual property is a way to build material wealth. Intellectual property and intangible assets work together to create economic value.

For the same reason, foreign enterprises and various companies made significant investments to enhance their property of intellect. The definition of "intellectual property" according to random house webster's unabridged dictionary is "property that results from original creative thought, as patents, copyright material, and trademark.

'Intellectual property' is the term that refers to the number of distinct types of formation of mind for which the stated property is recognized and the field of law is identified. Here, under this

¹⁷R.C. Cooper v. Union of India, AIR 1970 SC 564: (1970) 3 SCR 530

LegalOnus Law Journal (LLJ)

concept, the owners of that property are provided with certain exclusive rights to various types of intangible property such as artistic work, music, literature, inventions innovations, etc.

According to wipo¹⁸ works of literature, art, inventions, designs, names, symbols, and images used in trade are all considered forms of intellectual property (ip). Ip legally protects aspects like patents, copyrights, and trademarks, which allow people to profit financially or get notoriety for their inventions. The ip system seeks to create an atmosphere that encourages creativity and innovation by finding the ideal balance between inventors' interests and the public interest. Article 27 of the universal declaration of human rights, which guarantees the right to conservation of the material and moral interests deriving from the creation of works of literature, art, or science, outlines these rights. The importance of intellectual property was originally recognized by the Paris convention for the protection of industrial property (1883) and the berne convention for the protection of literary and artistic works (1886).

Since "intellectual property" refers to content that is a product of the mind or intelligence, its ownership rights are protected by the law in a manner comparable to that of other types of property. The main objective is to provide more funding for ongoing innovation to encourage when innovations are granted legal protection; it facilitates commercial transactions and fosters innovation and creativity. Because intellectual property rules vary from one place to another, obtaining, registering, or protecting ip rights requires individual efforts in each relevant location.

¹⁸ As per Article 2(viii) of the Convention Establishing the World Intellectual Property Organization (WIPO) Intellectual Property' shall include the rights relating to:

- literary, artistic, and scientific works;
- performances of performing artists, phonograms, and broadcasts;
- inventions in all fields of human endeavor;
- scientific discoveries;
- industrial designs;
- trademarks, service marks, and commercial names and designations;
- protection against unfair competition

And all other rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields.
WORLD INTELLECTUAL PROPERTY ORGANISATION, <https://www.wipo.int/wipolex/en/text/283854> (last visited on 20 No 2024)

LegalOnus Law Journal (LLJ)

The phrase "intellectual property right" (ipr) refers to a range of legal rights about specific types of knowledge, ideas, or other intangible assets commonly expressed in their expressive form. To modernize and enhance ipr management that prioritizes client satisfaction. Patents, utility models, industrial designs, trademarks, service marks, trade names, indications of source or appellations or origin, and the suppression of unfair competition, are protected under the Paris convention, 1967 (article 1(2)). When copyrights, geographical indicators, layout designs, and confidential information are included in industrial property, they all become intellectual property.

1.1 Different types of intellectual property

There are various forms of intellectual property i.e. The designs act defines a 'design' as the features of shape, configuration, pattern, ornaments, or composition of lines or colors applied to an article through any industrial process or means. The design must be novel and original, not previously produced, or reproduced, not disclosed to the public in India or outside the jurisdiction, and easily distinguished from other known designs. Once registered, the registered proprietor receives protection for an initial ten-year period, which can be extended for more years upon application.

The legal protection known as copyright gives someone the only authority to perform, translate, or modify a piece of copyrighted content. It may be acquired for computer programs, sound recordings, cinematograph films, and unique works of literature, theater, music, and art under section 13 of the copyright act. The original owner of the work is the copyright holder, who may grant other parties a license using a formal contract. In addition to, a lifetime of creator, published works are protected by copyright for 60 years.

The protection of plant varieties and farmer's rights act, 2007, aims to recognize the rights of Indian farmers and protect plant varieties to encourage their growth and development. India became a member of the trade-related aspect of intellectual property rights agreement (trips) in 1994, which requires all members to protect plant varieties. The act allows breeders, farmers, and authorized individuals to apply for registration of new plant varieties, which must satisfy conditions of novelty, distinctiveness, uniformity, and stability. Novelty requires the plant variety not to be sold

LegalOnus Law Journal (LLJ)

at the time of filing, distinctiveness requires a distinguishing factor from other protected varieties, uniformity requires all essential characteristics to be uniform, and stability means the essential characteristics must remain unchanged after repeated propagation.

A patent is an intellectual property right that protects a new invention and is granted for 20 years from the date of application. It is only registered if the invention is "novel" and "original," capable of industrial application, and requires "inventive steps" that involve technical advances or economic significance. The patents act grants each registered inventor certain rights, including the right to prevent third parties from using, selling, making, importing, or using a product without prior consent for a product patent and the right to prevent third parties from using a product obtained from a process patent without the original inventor's consent. The geographical indication of goods act, 1999: India's products, such as Darjeeling tea and Banaras saree, are popular due to their place of origin. Geographic indication (gi) is an indication that identifies goods as originating or manufactured in a specific territory or locality, with a given quality, reputation, or other characteristic attributable to its geographical origin. The gi act covers agricultural goods, foodstuffs, handicraft goods, manufactured goods, and natural goods. The trademark said "the shape of the goods, their packaging, and color combinations are examples of marks that can be visually represented and utilized to distinguish one person's goods or services from another. According to section 2(zb) of the trademarks act, this is what constitutes a "trade mark." to put it another way, a trademark safeguards terms, colors, shapes, and other components that are associated with or represent a product or service. Interestingly, trademark applications can be filed for marks that are planned for future use as well as for marks that are currently in use. The two main prerequisites for trademark registration are that the mark must be able to represent graphically and be able to differentiate the goods or services from those of others. A mark may be refused registration for the following reasons, according to the trademarks act: it lacks a distinguishing character, it is misleading and confusing to the public, it offends religious emotions; it is offensive, scandalous, or obscure, etc. Trademark registration is valid for 10 years, after which it may be extended for an additional 10 years if renewal applications are filed on time.

LegalOnus Law Journal (LLJ)

2. Trademark

Trademarks in India are governed by the trademark act, of 1999 which talks about the legal protection for symbols, brands, words, logos, or any combination used to distinguish one from other goods/ services. The word trademark includes any word, name, device, shape of goods, colors, or combination of colors used to distinguish it from the other products in the markets. The word trademark as defined under the section 2(1) (zb)¹⁹ where it stated that the mark was capable of being represented graphically and easily to distinguish it from other goods and services from other goods and services. Here, it means that there are three essentials required for the trademark that are:

- a. It requires to be a mark
- b. Capable of being represented graphically
- c. Should be capable of distinguishing its goods or services from the other goods or services.
- d. It may include goods, the shape of goods or packaging, and colors or a combination of colors.²⁰

A combination of elements that distinguishes one company's goods or services from those of another is called a trademark. It falls under the ambit of one type of intellectual property and it is also recognized by both international treaties and national laws. The line as Nike and McDonald are some examples of the trademark.

¹⁹a mark capable of being represented graphically and which is capable of distinguishing the goods or services of one person from those of another and may include the shape of goods, their packaging, and combination of colors and: -

(i) About Chapter XII (other than section 107), a registered trademark or a mark used about goods or services to indicate or to indicate a connection in the course of trade between the goods or services, as the case may be, and some person having the right as proprietor to use the mark; and

(ii) about other provisions of this Act, a mark used or proposed to be used about goods or services to indicate or so to indicate a connection in the course of trade between the goods or services, as the case may be, and some person having the right, either as proprietor or by way of the permitted user, to use the mark whether with or without any indication of the identity of that person and includes a certification trade mark or collective mark.

²⁰ Section 2(1)(i)(ii)(zb) Trademark Act, 1999(Act No.47 of 1999)

LegalOnus Law Journal (LLJ)

2.1 Marks

According to the trademark act of 1999, section 2(1) (i) (v) (m), a mark is "a device, heading, brand, label, name, letter, numeral, signature, word. Here, the term mark also includes the "shape of goods, packaging or combination of colors or any other form of combinations".

- Certificate trademark: the owner usually uses these marks to attest to the origin, composition, quality, manufacturing process, or service delivery, among other attributes of the goods or services to which they are applied. Two examples of authorized marks are the ISI mark, issued by the bureau of Indian standards (BIS), and the Agmark, issued by the government of India's director of marketing and inspection.
- Collective trademarks: the trademarks we have previously examined are not the same as this one. An organization or association of members usually uses this kind of mark to set its members' goods and services apart from those of non-members. The CA mark, restricted to registered members of the institute of chartered accountants, is a well-known example of this kind of trademark.
- Product mark: this mark is used for goods and products, but not for services. It is used to denote the product's origin, reputation, and supplier. Trademark applications submitted under class 1-34 the term "product marks" is commonly used to refer to the fourth trademark rules of 2002.
- Smell mark: a small number of trademarks registered under this category have received international registration. However, in India, a mark needs to be able to be visually depicted to be considered a trademark. The public should be able to recognize and identify such a representation. Furthermore, a functional odor is not eligible for registration. In addition, odors that are descriptive or functional are ineligible for registration. A perfume that has a nail polish remover added to cover up the chemical odor, for instance, can be considered useful. Additionally, a scent that arises naturally from a mixture of components cannot be protected as a trademark. If a trademark application of this kind can pass these requirements and prove distinctness they can be registered.

LegalOnus Law Journal (LLJ)

- Service mark: despite looking like a product mark, this mark is only used to distinguish services, not products. Applications for trademarks in classes 35–45 are filed. Pultes 1002, which is included in the fourth schedule to trade marks, may be considered a service mark.
- Device mark: a device mark usually consists of an artistic element, like symbols or a pictorial or artistic depiction, in addition to the word mark element. It typically includes a word mark together with a number of artistic elements. These elements of a device mark could include both non-trademark able and trademark able traits. This kind of mark protects the registered composite mark but not for the individual components. It's interesting to note that a device mark's protection is restricted to the color combination in which it is registered. However, a black-and-white registered device mark offers more protection, allowing the owner to claim color protection for the device registration.
- Word mark: usually, a word mark or device mark is used while registering a trademark. Without any additional artistic components or stylization, a word mark simply uses a word or text to indicate a trademark. Because it permits the owner to use the mark in any style, form, or depiction, this sort of registration offers a trademark the broadest legal protection. Examples of registered trademarks include Coca-Cola and little hearts.
- Sound mark: when registering a trademark, graphic representation is crucial, and this also holds for sound markings. A sound must be unique and recognizable to the consumer to be registered under the trademark. According to the tm manual, several types of sounds are expressly not allowed to be registered as sound marks. They are as follows: tunes that serve as chimes, simple musical compositions with just one or two notes, children's nursery rhymes, music that is closely linked to a specific area, and popular music.
- Color trademark: they are protected as a trademark as the trademark act of 1999 defines a trademark as "a combination of colors." to be registered as a color mark, nevertheless, such a combination of colors needs to be original, distinctive, and able to identify the product and its source. Orange will not be distinguished by a straightforward red-and-yellow combo. Customers must be able to recognize the color for it to be registered under this kind of trademark e.g. Cadbury.

LegalOnus Law Journal (LLJ)

- Shape trademark: "shapes of goods" are utilized by the trademark act of 1999's definition of a trademark. Thus, the trademark act of 1999 also protects form marks. Section 9(3) of the act does, however, contain a restriction that specifically prohibits the registration of a trademark that solely consists of shapes derived from the actual nature of the goods. Forms that are required to achieve a technical outcome. Shapes that significantly increase the goods' worth. Furthermore, when such an application is made, it should be related to the items rather than the goods' container.

2.2 historical background of trademark

A trademark can protect a word, phrase, logo, design, symbol, or combination of these. It gives a product that symbolizes a supplier of products or services a unique identity. In India, a trademark is protected by both common law and the trademark act of 1999.

The traces of trademarks found back to the onset of the industrial revolution which led to the large production of goods and distribution of goods at the same time. In the emerging times of competition in a market economy, the manufacturers started to address their goods by some specific marks, and symbols, so to distinguish their goods from the other market goods. Also, the manufacturers of the goods started advertising their products by their own created marks in the market. Here, the necessity of marks is raised. The necessity for the protection of goods and the reputation in the market is felt in all nations. So, for the first time at the international level Paris convention was adopted in 1883 for the protection of intellectual property.

Before the law of trademarks was recognized by the statutory, the equity court started to give some reasonable protection. Here, the owners of trademarks have the right to file a complaint suit against such infringement. The owner of the trademarks was tried by the court of equity which granted appropriate reliefs. The first trademark law to be added to the Indian statutory book was the merchandise marks act of 1889. The trademark act was enacted in 1940 as a result of the issues with the said act, which was followed by the trademark act. Before the enactment of said trademark act, 1940, the issues relating to the infringement of trademark or the passing off were considering

LegalOnus Law Journal (LLJ)

section 54 of the specific relief act were get decided and whereas the issues relating to registration of the trademark were decided by the Indian registration act, 1908.

Before the independence of India, the first protection to trademark was given through the trademark act, of 1940; the act was specifically based on the England act of trademark 1938. The trademark act of 1940 established the registration process of trademarks and it also gives statutory protection to the trademark which was registered by law. The trade and merchandise marks act of 1958 repealed the Indian merchandise marks act of 1889 and the trademarks act of 1940. In 1958, the trade and merchandise marks act were passed. The 1940 act was superseded by the trade and merchandise marks act of 1958 in India. This new law had more detailed rules for trademark protection, including handling infringement and imposing penalties. India's decision to join international agreements, such as the Paris convention for the protection of industrial property in 1998 and the agreement on trade-related aspects of intellectual property rights (trips) in 1995 required the country to update its trademark laws to meet global standards. This resulted in significant changes to domestic laws, ensuring better protection for trademarks and a commitment to international intellectual property rights principles. Section 129 of the act stated that a mark that purported to or declared the ownership of a person's title to a trademark other than a registered trademark was not to be registered under the Indian registration act, of 1908. In other words, section 129 talks about the capability of registration of trademark which to be registered or not.

The act of 1958 did well for 4 decades. However, considering the development of business and trade practices, as well as the increasing globalization of trade and industry, the need to encourage investment flow, and technological advancements and transfers, it is necessary to standardize and streamline the trademark management system and give judges' decisions weight. Here, the necessity of changes and harmonization of trademarks increased due to various changes in the world even in technology and globalization of trade and industry. Digitization and online databases have further enhanced the transparency and user-friendliness of the process. India's trademark journey has been significantly impacted by the establishment of the intellectual property appellate board (ipab) and its accession to the madrid protocol in 2013. The ipab has been instrumental in

LegalOnus Law Journal (LLJ)

resolving trademark disputes and ensuring fair decisions. The Madrid Protocol has allowed Indian businesses to register and manage their trademarks internationally, simplifying global brand protection efforts. Further, India becomes a party to the most important agreement i.e., TRIPS (agreement on trade-related aspect of intellectual property right). This act created a strong legal foundation for trademark protection in India by introducing measures for trademark registration, enforcement, and infringement protection. Over time, efforts have been made to improve and refine trademark procedures, making them more efficient and accessible. So, after that, the Trademark Act, of 1999 was established which later came into force on 15 September 2003. In 1883, India ratified the Paris Convention on Intellectual Property Protection. The 1958 Trademark Act was later repealed by the 1999 Trademark Act. Now the new Trademark Act, of 1999 has also been confirmed at the international level and has been accepted by both treaties at the international level. The Trademark Act of 1999 was a milestone in India's trademark law history, bringing together and modifying laws related to trademarks, aligning them with the obligations of TRIPS. Key features included the introduction of service marks, recognition of "well-known" marks, provisions for protecting registered users, tougher penalties for trademark infringement and counterfeiting, and a simplified trademark registration process. These modifications strengthened and improved the effectiveness of India's trademark laws, guaranteeing improved trademark protection and promoting economic development and innovation. The trademark remedies are also not available only for trademark law but also for the remedies for unregistered trademarks under common law.

The Trademark Act of 2003 is a significant revision of existing trademark laws in a country to improve protection for trademarks, which are essential assets for businesses. This may involve modifications to registration procedures, expanding eligible trademark scope, or stronger measures to combat trademark infringement and counterfeit goods. The act aims to strengthen the legal framework governing trademarks, safeguarding the interests of businesses and consumers. The Trademark Act of 2017 continues this tradition by modernizing and adapting trademark laws to meet emerging challenges, including digital-era regulations.

LegalOnus Law Journal (LLJ)

2.3 objective and functions of trademark:

Trademark law serves two fundamental principles. Which is by distinguishing the source or origin of specific products as distinct from other comparable products, and other is to protect the public from confusion and deception; also, it defends the trade and commerce of the trademark owner and the goodwill associated with his brand.

According to the Delhi high court's ruling in Cadbury India limited v. Neeraj food products²¹, the goal of trademark law is to safeguard consumers and traders from dishonest trademark adoption by third parties seeking to profit from goodwill and reputation.

The primary functions of the trademark are that it allows one trader's wares to be identified and set apart from those of other traders, it indicates that a certain trademark is the source of all items carrying that mark, it indicates that goods displaying that mark are of the same caliber and serves as a key tool for product sales and promotion. As a result, its key features are advertising, quality, source, and identification.

2.4 significance and benefits of trademark

Trademarks are essential for a company's identity, connecting it to consumers through its name, design, and colors. They convey a product's standard and quality, preventing confusion and potential loss of reputation. Trademark registration protects a company's reputation by preventing manufacturers from using the same name and logo on cheaper products. Consumer protection is another benefit, as trademarks prevent confusion about the brand. Long-standing trademarks, like the Belgian beer brand stella Artois, strengthen market footing. Financial benefits include adding value and recognition, making it easier to raise money, and facilitating partner and collaborator finding.

²¹Cadbury India Limited v. Neeraj Food Products, 142(2007)DLT724, MIPR2007(2)269, 2007(35)PTC95(DEL)

LegalOnus Law Journal (LLJ)

Trademark registration offers several benefits, including exclusivity, legal protection against infringement, differentiation from competitors, goodwill and brand value, creation of an intangible asset of value, global recognition and eligibility, cost-efficient protection, and attraction of new customers.

- Exclusivity allows the owner to use the same trademark for every item that falls under the specified classes, preventing third parties from advertising similar services or products using confusingly identical trademarks. Legal protection against infringement is provided by assigning intellectual property to the product, which can be used without permission by any third party. The owner can use the ® symbol to indicate exclusive rights and can seek redress in court from infringement.
- Differentiation from other products is another benefit of trademark registration. A unique trademark sets a product apart from its rivals, forming a customer base and impacting buyer decision-making. A registered trademark enhances the company's image in the market by maximizing consumer confidence.
- A registered trademark creates an intangible asset of value, acting as a source of income in aspects like income tax or accounting. It can be sold, bought, licensed, assigned, used commercially, or franchised, and its economic value increases with business growth and popularity.
- India, as a signatory to the Paris convention for protection of industrial property, has the right to secure registration and protection of their trademarks in countries that are signatories to the convention. This registration and goodwill can act as a strong foundation for international recognition.
- Cost-efficient protection is another advantage of trademark registration. In India, a registration can be renewed on time and is valid for ten years after the day the application was submitted. Online registration is a convenient and cost-efficient process, generally issued within a few days after filing.

LegalOnus Law Journal (LLJ)

2.5 need for protection of trademark

A trademark is a unique symbol or design that differentiates a company's products or services from others, serving as a brand's signature. It enhances visibility, customer loyalty, and overall value. Customers can connect with products through trademarks, overcoming language limitations. A consistent, recognizable trademark builds trust among consumers. Trademark registration typically lasts ten years, with renewals available for an additional fee. In India, trademark protection is enforced through court orders, extending to registered and unregistered trademarks.

The trademarks act of 1999 safeguards trademark rights in India. After India signed the TRIPS (trade-related aspects of intellectual property rights) agreement, the act was primarily implemented to fulfill India's international commitments. In India, who has been using a trademark for the longest time determines who owns it, in contrast to patents and other forms of intellectual property rights. Consequently, the "first-to-use" notion replaces the "first-to-file" concept in terms of trademarks.

- Trademark infringement happens when another party uses a mark that is confusingly like a registered trademark for related products or services, potentially generating confusion or eroding the brand's distinctiveness. It could be either a direct or indirect infringement. Trademark owners must safeguard their marks and take legal action against infringers. The only defense can be that they had prior registered, fair use, and the owner had not renewed the trademark over a long period after expiry. Key aspects of trademark infringement and enforcement include cease-and-desist letters, litigation, and defenses such as fair use, parody, or generalness. If a cease-and-desist letter does not resolve the issue, trademark owners can file a lawsuit in federal court, which may include injunctive relief, damages, and attorney's fees. Trademark registration: you can establish your ownership rights and obtain legal protection by registering your trademark with the relevant intellectual property office. By acting as a public notification, registration discourages unauthorized use and facilitates the enforcement of your rights in the event of a violation.

LegalOnus Law Journal (LLJ)

- **Vigilance and monitoring:** keep an eye out for possible trademark infringements in the marketplace. To find identical or similar marks that could threaten your brand, regularly search for trademarks. Taking quick action can improve your legal standing and stop additional harm.
- **Protect your rights:** act quickly to protect your rights if you find trademark infringement. Sending cease-and-desist letters, holding talks, or pursuing legal remedies like injunctions and damages could all be part of this.
- **Inform clients:** inform clients on the importance of your trademark. By increasing knowledge, you can reduce the possibility of confusion by assisting customers in differentiating your goods or services from those of infringers.
- **Consider alternative dispute resolution:** in certain situations, trademark disputes can be settled without the need for expensive litigation by using alternative dispute resolution techniques like mediation or arbitration.

Business owners may preserve their brands, keep their competitive edge, and guarantee the ongoing strength and integrity of their trademarks by comprehending the nuances of trademark infringement and putting these preventative steps into place.

2.6 trademark registration process and regulations

- i. **Trademark search:** make sure your suggested trademark is original and has not been registered by someone else before deciding on one.
- ii. **File an application:** send a trademark application, together with the necessary paperwork and payments, to the Indian trademark office either online or offline. It must be submitted online using the official websites of the controller general of patent design and trademarks, the department of industrial policy and promotion, and the ministry of commerce and industry (agents, attorneys, or the proprietor/applicant may all register).
- iii. **Examination:** to make sure your application satisfies legal requirements, such as distinctiveness and trademark rule compliance, the trademark office will review it.

LegalOnus Law Journal (LLJ)

- iv. Publication: if the trademark is approved, it will be published in the trademark journal for four months to accommodate any objections from third parties.
- v. Opposition (if applicable): parties have the allotted time to object to the registration if they have any.
- vi. Registration: a registration certificate will be provided and the trademark will be registered if no opposition is lodged or if opposition is unsuccessful.
- vii. Renewal: by paying the renewal costs, trademarks that have a ten-year validity period can be extended forever every ten years.

The trademark act of 1999 and the trademark rules of 2017, which were created by the act, are the main laws governing trademarks in India. Procedures for trademark filing, examination, publication, objection, registration, renewal, rectification, and removal are listed in the act and rules. Like patents, the chief administrator of the Indian trademark system is the controller. The general of patents, designs, and trademarks (cgpdmt) office is managed by the department of industrial policy and promotion (dipp), ministry of commerce and industry. From trademark search to trademark registration and subsequent renewal, there are numerous procedures involved in the effective registration of a trademark. Every step entail completing the necessary paperwork and procedural procedures.

2.7 trademark licensing:

The trademarks act, of 1999 does not define "licensing of tm." a trademark license is permission granted by the owner of a trademark to a third person in consideration of a royalty. The holder or proprietor of the registered trademark can grant a trademark license. Both registered and unregistered trademarks can be transferred under Indian law through licenses or assignments. Licenses to a registered trademark in India can be simple license agreements or registered users, with certain rights granted to the licensee.

According to section 49 of the trademarks act 1999, it is a person who is currently registered as such. Section 49 of the act requires the owner of a mark and a proposed user to jointly apply for a

LegalOnus Law Journal (LLJ)

registered user to use the mark. The application is made in form tm-u, containing an agreement and an affidavit from the proprietor detailing the license details. The application must be submitted within six months of the agreement. The official online application cost for each mark is rs 4500. If the application is approved, the trademark office (tmo) would register the user as a registered user and publish it in the journal.

Himalaya drug co.pvt.ltd, Bangalore v. Arya aushadhi pharmaceutical work Indore²², the court decided that a company might have its lawsuit dismissed if it couldn't demonstrate that it was a registered user. Therefore, registering the tm license with the trade mark office is always a good idea. According to the trademarks act of 1999, only a registered trademark owner or proprietor is authorized to commence legal action for trademark infringement; a non-registered user is not permitted to seek legal action under the act.

2.8 trademark strategies:

An effective company's brief trademark strategy should align with target customer demand and interest, ensuring it is marketable and associated with quality and satisfaction from products and services. A trademark strategy is crucial for a company's uniqueness and should be distinct, definable, and recognizable. Key points for developing a trademark strategy include the registration process, marketing of the trademark, and protection from competition.

Registration grants exclusive rights to use the trademark across the jurisdiction for 10 years, and renewal is essential to maintain rights. Keep the trademark description broad and avoid using a logo without a color claim. Marketing of the trademark involves connecting the brand, product, and services with potential customers. Registering a domain similar to the trademark can prevent others from obtaining it. Conducting market research and conducting surveys can provide valuable

²² HIMALAYA DRUG CO.PVT.LTD, BANGALORE V. ARYA AUSHADHI PHARMACEUTICAL WORK INDORE, AIR1999MP110, AIR 1999 MADHYA PRADESH 110, (1999) 2 ARBILR 528

LegalOnus Law Journal (LLJ)

insights for creating a compelling trademark. A strong trademark strategy can help protect the brand, products, and services from competition and provide a competitive advantage. For example, MacDonald had created their logo registered and restricted other persons in the market from using their logo and had created their brand. In jurisdictions with exclusive rights, write the registered trademark with a circled "®" and in those without exclusive rights, write tm.

Trademark portfolio management

Trademark portfolio management is the strategic administration of a company's trademarks to maximize their value and protection. It involves choosing the right mark, conducting thorough clearance searches, registering trademarks, conducting portfolio audits, enforcing and protecting trademarks, and managing renewals. Key components of trademark portfolio management include choosing the right mark, conducting thorough clearance searches, registering trademarks, reviewing and assessing the portfolio, enforcing and protecting trademarks, and managing renewals.

To ensure effective trademark portfolio management, align trademark decisions with the overall brand strategy, centralize portfolio management, stay proactive, invest in education and training, and engage the right partner. A centralized system or software solution can streamline the process, while regular monitoring of trademark databases, industry publications, and online channels can help identify potential infringements or misuse. Investing in education and training can also help employees understand the importance of trademark protection and uphold brand integrity. Partnering with experienced trademark attorneys, ip professionals, or service providers can provide valuable guidance on portfolio strategy, enforcement actions, and compliance with relevant laws and regulations. To protect important brand assets, trademark portfolio management is a complex process that calls for proactive oversight, smart decision-making, and meticulous preparation. Businesses can strengthen their market position, improve brand reputation, and open up new growth prospects in a more competitive business climate by implementing best practices and maintaining vigilance in trademark protection.

LegalOnus Law Journal (LLJ)

3.1 trademark: contribution to market distinctiveness

Here it was stated that the trademark's primary role is to distinguish the business goods and services from the other goods and services of competitors. In the trademark, by providing a unique identity to the goods or services through name, logos, slogan, etc. It ensures that it is distinguished from the other competitors and makes it easy for the consumers to recognize the origin of that product/goods or services. The source identification is the main basic point for the trademark to help in market distinctiveness and it builds consumer trust and loyalty with the specific product trademark. The expression "distinctiveness" means to state that the adapt it to "differentiate with which the proprietor was connected". It would be suggested that if the trademark was not distinct the product that not liable for the registration of a trademark. Here, it also says that the trademark allows the business to create distinct identities for their goods or services, which helps the consuming consumer to differentiate it from competitor things and to prefer their advantages. The imperial tobacco co. Of India ltd. V the registrar of trade marks²³, here the court of Calcutta said that distinctiveness means to be "some quality in trademarks marked to the goods so marked as distinct from the others producers of such goods". A strong "well-known" trademark can evoke an immediate need for brand recognition through the trademark, to make it easier for the consumer to make their decision regarding the products or services. Just like Nike and coca-cola is easily recognizable by the consumers of their logo and designs and it creates loyalty among the consumers. The word well-known trademark means to be a mark that becomes a substantial point to the public here which it used goods and services that such use of such mark about such products would be taken as indicating a type of connection between trade or rendering of services between those products and the person using such mark about that services or goods.²⁴ in the case of yahoo inc. V. Firoz Nadiadwala²⁵, the court stated that yahoo has become the common name in all

²³ The Imperial Tobacco Co. of India Ltd. v the Registrar of Trade Marks AIR 1977 Cal. 413

²⁴ Section 2(1)(zg)

²⁵ Yahoo Inc. v. Firoz Nadiadwala CS (OS) No. 906/2009

LegalOnus Law Journal (LLJ)

households in India and now it achieved the status of well- a well-known trademark for a very long time it has continued nowadays, and here the defendant using yahoo making a film and believing the public the defendant production was same endorsed and associated with the plaintiff.

In the competitive world, there are more challenges faced by the new companies which newly launch their new product. So, in a competitive market with almost the same products, here the trademark gives a new identity to the goods or services of that business to differentiate it from the other business products in the crowded workplace. The differentiation and distinctiveness play a very crucial role in the differentiation of the product and in attracting customers. For example, Samsung and apple phones are the best examples of distinctiveness in the market; they have their own different characteristics identity despite being similar types of products. Later, the time after ages the trademark was associated with the quality assurances and the trust of consumers. A strong trademark symbol, logos, symbol, word, etc. Assures consumers that they purchase have certain standards. When the customers purchase something by having their trademark it assures the consumers about the quality and have good experience with them.

Trademark leads to market efficiency by reducing the time and effort of consumers spending so much time over the purchasing of goods or services. Here, the feature of a trademark gives a product a label and mark which gives its unique identity to that product, it makes it easy for the consumer to easily find that product in the market instead of spending much time and effort for searching the products. Here, it helps to evaluate all the products separately, here the consumers rely on the trademark of the products and value the products. It also helps in reducing confusion or other malpractices in the marketplace, since the trademark specifically leads to the branding of the product. The trademark helps the business carve out market inefficiency by giving and reinforcing the unique identity of the product by giving or representing by brand name. A distinctive trademark and the branding are coupled together and work accordingly. It allows the business to establish a specific market by minimizing the direct competition in the market. For example, here the most important ones louis Vinton and monte Carlo are the most famous brands and high-end exclusive brands, preventing them from the mass- market products. The trademark

LegalOnus Law Journal (LLJ)

contributes to the creation of brand equity. A successful trademark leads to more benefitted market profits for the company, consumer attraction, and consumer loyalty and the increasing value of that brand in the world. Here, to testing the parameters of the testing for the distinctiveness of a trademark are – the extent and how much period it was used, goodwill and association are set in the mindset of the consumer, investment is done on advertising, channels of distributing it, and the class of consumers approached.²⁶ so the trademark enhances the market distinctiveness by giving a unique identity to its products through brands and consumer loyalty, consumer recognition enhancing the business of the company and differentiates it from the other competitor products. Here, the trademark becomes the most valuable asset for the business to establish a brand presence in the world.

3.2 concept of branding in the trademark

In today's era, the trademark serves as an important tool for businesses to protect and establish their brand identities. It helps in distinguishing it from the other competitor products enabling consumers to easily purchase the things. It helps in fostering consumer confidence, brand recognition, and brand loyalty. So, in today's time, it is easy and more trustworthy to purchase branded things instead of others. A trademark is granted by laws and is legally protected, whereas a brand is the name or logo that was provided by the product's owner. A brand²⁷ is specifically a name given to the product by the owner who manufactured that product. It is the name of the product that symbolizes the company's products and leads the consumer to purchase such branded products. A "brand name contains the elements such as culture, picture, identification, and spirit of the company. It is generally used to distinguish it from the other products". However, the brand name should be given before it to introduce in the market. The word brand can be defined as "it is

²⁶ Kunj Aluminium Private Ltd. v. Koninklijke Philips Electricity NV, 2011 (47) PTC 472 (Del)(DB0)

²⁷ Chapter 9 of the Central Excise Tariff Act, 1985, is as follows-

"A brand name or trade name, whether registered or unregistered, is a name or a mark, such as a symbol, logo, tag, signature, or created word or writing, which is used about any specific commodities for denoting, or indicating, a correlation in the course of a business between such specified goods as well as some individual using such name or sign with or without any indication of that particular personality."

- Central Excise Tariff Act, 1985, No. 5, Acts of Parliament, 1985 (India)

LegalOnus Law Journal (LLJ)

the name assigned to a specific product by the firm that manufactures it"²⁸. Also, according to the dictionary, it is defined as an "it is term, sign, name, etc., specifically one officially registered as a trademark, which is used by a producer or the trader to distinguish its items from one another for the same sort and is prominently displayed on its products, in marketing, etc."

The term 'brand' or 'brand' was established from the early Norwegian word which means "to burn or to set alight". It dates back to the time when sheep were marked by shepherds to help them too distinct it from one another. This was done by burning a distinguishing mark into the sheep using the iron. The term was later adopted by English and the later the term was originally used to describe the owner, creator, or source of the thing. Here, the brand name serves two main purposes i.e., identification which means that it helps to distinguish it from another similar type of good or service, and the other purpose is the verification of the products, which means it helps to confirm the real identity of the item. Here, the brand name reveals the brand purpose of the product. It helps in establishing the business in the market by the strong brand identity name and to target the audience and to attract the attention of consumers. Before establishing or introducing the product in the market, it is essential to establish it by brand name to distinguish it from the other products.

4. Anticompetitive effects of trademark

Trademarks on the one hand are intended to promote competition by fostering market distinctiveness; there are instances where they can have anticompetitive effects. This occurs when trademark rights are used to restrict competition unfairly, hindering the entry of new business into the market or limiting consumer choices.

There is one concern is the use of trademarks to create market barriers. This can happen when a dominant brand uses its trademark to prevent competitors from using such similar marks, even if those marks are not confusingly similar to the original. For instance, a well-established brand

LegalOnus Law Journal (LLJ)

might try to prevent new entrants from using similar types of marks, even if their products are different.

So, in this case the trademark under some forms leads to competitive effects, particularly when the other uses that limit competition. On the other trademark, means to protect the brand and identity leads to antitrust concerns like:

Market barriers are when the dominant brand uses its trademark to prevent competitors from using similar marks, even if those marks are not similar. A strong recognizable trademark creates a strong identity in the market that leads to stopping new entrants. Established and brand recognition by marks made it difficult for the new or smaller business to compete in the market and enter the market.

Brand loyalty works as a barrier for new businesses. When the trademark becomes the first priority for the person, in short, the consumer wants to prefer the trademark-branded sites or products. For example, google was the priority for the search engines. Trademarks can grant exclusive rights to a particular brand, potentially restricting the use of similar marks by competitors, even if the products or services are different.

Tying arrangement and bundling, here the dominant firms with the strongest trademark tie up and bundle with the other for the same offering. Here, the customers are required to purchase the things along with the additional products. Here, it works to force consumers to remain specified or with the same brand and prevent them from other alternative products or brands. Here, in the process of branding the dominant brands are bundled with the well-known trademark products with the less competitive items, trying to reach the other market segments. Here, in short, it tries to limit the consumer's availability and create barriers for other new companies/ businesses.

Brand extension, it is expanding a trademark to cover unrelated products or services, potentially limiting the competition in the new market. Here, the dominant brand names extend the trademarks with the multiple types of product categories, by limiting or stopping the opportunities or creating barriers for the smaller business in the markets. Thus, it limits the competitor's ability to

LegalOnus Law Journal (LLJ)

differentiate and forces the new business to enter the market without the same trade dress or brands that could market position.

Monopolization of power in the market of trademark. If the strong protection of trademarks was enforced very broadly, lead to monopolistic practices. It refers to the point where the business used the trademark of the rights of their products to exercise their excessive control over the market, beyond the limit of the simple protection of their trademark, in that scenario it limits the competition and reduces consumer freedom of choice of products and leads to monopolistic effect. Some companies bring suit against the similar sounding marks even in the unrelated markets where they work in the other sector. This type of act prevents other businesses or companies from using common words or names for their businesses. In some cases, where the trademarks are used to prevent the competitive products from gaining the same reputation or recognition, here it limits the consumer choice of products. A monopolistic trademark power is used to excessive use of power to limit the diversity of business into the market. It leads to something reduced in quality or higher in price due to the lack of competition in the market.

In the case of Starbucks corporations v. Sardarbuksh coffee & co.²⁹, here the most famous Starbucks registered their mark with the name of "Starbucks" which is famous for the coffee and in India as a trademark in the year 2001. On the other side, the defendant started the business in 2015 under the given name, it was associated with the turban commander's face with the wavy lines surrounded by the circular black band. Here, the plaintiff requested the change of the logo of the defendant's mark. Here, the defendant also changed the logo and started the business. Here, the plaintiff filed a suit against the defendant for the infringement of a trademark on the grounds of the deceptive similar marks. Here, the Delhi HC relied on the facts and cases.³⁰ stated that to find the deceptive nature of the defendant the court has to put in the shoes of the customers to

²⁹ Starbucks Corporations v. Sardarbuksh Coffee & Co., CS (COMM) 1007/2018

³⁰ National Sewing Thread Co. Decision Ltd. v. James Chadwick & Bros. Ltd., 1953 AIR 357, 1953 SCR 1028, AIR 1953 SUPREME COURT 357, 1956 BOM LR 21

LegalOnus Law Journal (LLJ)

differentiate it or not. The court held that the ordinary man was confused with the same marks and so it comes under the deceptive similar marks.

In the *mondelez India foods private limited v. Neeraj food products*³¹, in this case, the plaintiff (Cadbury India limited) filed a suit against the defendant on the ground that the defendant has the same deceptive identical mark and products. The plaintiff filed a suit on the basis that the defendant sold chocolates with the mark name 'James bond' which is the same mark as the Cadbury gems. Here, it also tries to confuse the market and consumer's mind. Here, the court held that the plaintiff was correct with the point and awarded the damages of rs. 10 lakh from the defendant.

4.1 antitrust implications of branding strategies

Branding strategies can have significant antitrust implications, particularly when they involve practices that restrict competition or create unfair advantages. Antitrust authorities closely examine branding strategies to ensure they do not violate antitrust principles.

For example, anti-competitive branding strategies can include:

1. Exclusive dealing agreements: restricting distributors or retailers from selling competing products or services.
2. Tying arrangements: requiring customers to purchase a product or service only in conjunction with another product or service.
3. Predatory pricing: it is the practice of lowering prices to drive out rivals.
4. Monopolization: using dominant market power to restrict competition unfairly.

4.2 consumer protection and trademark law

³¹ Mondelez India Foods Private Limited v. Neeraj Food Products CS (COMM) 393/2018

LegalOnus Law Journal (LLJ)

Trademark law serves a vital role in protecting consumers from deception and confusion in the marketplace. By ensuring that trademarks accurately indicate the source of goods or services, consumers can make informed decisions, confident that they are purchasing products from the intended source. This protection is essential for maintaining consumer trust and confidence in the market.

A key aspect of consumer protection is preventing trademark infringement. This occurs when someone uses a mark that is identical or confusingly similar to a registered trademark without authorization. Trademark infringement can lead to legal action, as it undermines the value of the trademark and can confuse consumers. By prohibiting infringement, trademark law safeguards the integrity of the marketplace and ensures that consumers are not misled by counterfeit or unauthorized products.

Here, both the words consumer protection and trademark law are intertwined because they both aim for consumer protection and access to the most appropriate information and to protect them from misleading or deceptive practices. Section 3 carries the exception that deals with the protection of intellectual property rights. Section 3 of the competition law deals with the situation in which the section does not deal. This sub deals with the parts that do not restrict the right of any infringement of any ip rights. The rights of the protection of these rights can't be waved off. The section lists some of the acts in which rights are enshrined. These are copyright law, patent law, trademark law, geographical indication, and the design act.

It is said that ip rights are not used in that manner which brings a competitive outcome. These ip rights are granted for the exclusive use of the product without any third-person interference. This was used as a method of enabling the process of invention and creativity to be awarded to be used. So, the state is concerned with safeguarding the consumers and the markets from the exclusive use of marks. So, the intellectual property law and competition law are not reconciled together. The competition was established to prevent abusive use of ip rights.³²

³² Flughafen Frankfurt/ Main AG, 98/190: (1998) OJ L72/31, para 89

LegalOnus Law Journal (LLJ)

Brand names are intended to assist buyers in recognizing the source of the products by safeguarding the distinctive name, logos, images, and other identities of the brand. This security allows the purchaser to settle on informed decisions, realizing the item with the specific brand name comes from a particular source with a certain quality and notoriety. By preventing the unapproved utilization of the trademark, trademark law regulations limit the consumer's disarray about the item's origins. This could help the customers with the trademark and product trust. Nike is truly the best example for limiting the confusion of customers.

Here, it also talks about the assurance from the fakes and extortion. It means that the fake products which are frequently of substandard quality, can hurt the buyers from both perspectives i.e. Financially and physically. The trademark law protects the consumer by forbidding the offer of fake items. This shields buyers from unconsciously buying inferior quality or perilous items that abuse a reputed brand trademark. Through trademark law enforcement, companies can take legal action against the people who utilize their brand trademark without their consent, lessening the availability of phony merchandise and guaranteeing that customers are buying real brand products.

Trademark law assists with preventing deceptive show casting, where a brand could utilize a logo, or name, that looks the same as those of notable brands to mislead the consumer into buying that product. Such practices are known as compromising the trade dress or passing off of trade. By confining that type of activity trademark law assists the consumer with the avoid such buying impersonation items that don't satisfy the quality standards of them which they expect from the brand. The trademark law supports consumer trust by permitting the brand to assemble the notorieties because of the consistent quality of the product. At the point when the customer sees a perceived trademark brand, they partner it with a specific level of quality of product and build steadfastness. This consistency benefits the consumer who purchases the products based on confidence in the product. Without the trademark protection law, it would be difficult for the companies it would be difficult to maintain their reputation and its value and its consumers. The trademark allows for fair competition in the market by using the distinctiveness of the product and by preventing others from using the same brand name to prevent consumers from getting confused.

LegalOnus Law Journal (LLJ)

In the competitive world, consumers must benefit from the various goods, prices, and quality levels of the products.

4.3 trade dilution about the brand equity

Trade dilution deals when a well-known trademark owner has the right to forbid others from using their mark because it diminishes their exclusivity or damages their reputation. This is known as trademark dilution, which is a type of trademark infringement. In actuality, nobody has the authority to misuse a well-known trademark's reputation or copy it. Dilution protection, on the other hand, is meant to keep a sufficiently powerful and well-known trademark from losing its exclusive identification with a specific product in the minds of the general public.

The Indian trademark dilution doctrine: although dilution is not defined in the trade marks act, 1999, section 29(4) declares that if a trademark is well-known in India, using a mark that is close to or identical to the registered trademark for goods or services that are not the same is deemed to be an infringement. This is because such use without due cause would unfairly exploit the reputed trademark or harm its distinctive character. The act postulates that a registered trademark is infringed when a person takes undue advantage of an eminent mark or mark with a distinctive character. The term trademark dilution refers to the erosion of a trademark's distinctiveness and value, even in the absence of direct confusion with another product or service. This can occur when a trademark is used in connection with unrelated goods or services, potentially it harms or tarnishes the brand's reputation or erode the value in the consumer's eyes. The trademark dilution significantly impacts the brand's equity which is used to represent the intangible value lingered with the trademark. Brand equity encompasses factors such as brand awareness brand quality brand loyalty and the association with some emotions or the value of the brand. When the trademark is diluted, it leads to a decline in the brand equity by harming a business's reputation. Here it was also stated that when another business uses an identical mark that leads to diminishing the uniqueness of the brand's trademark eventually it harms the reputation of the brand in the mind

LegalOnus Law Journal (LLJ)

of the consumer here the option to start the legal proceeding for safeguarding the trademark from the dilution. It also becomes challenging when the trademark is diluted, making it difficult for the brand owner to prove its unauthorized use of the mark. So, the major step for safeguarding the trademark from dilution is to enforce and protect the brand. To watch out for the unauthorized use of that trademark, informing the customers about the dilution and uniqueness of the brand name, the next step is to licensing and merchandise agreements to be done for the correct usage of the trademark and the last one is to register the trademark and enforce the legal proceeding against the unauthorized user.

5. Balancing trademark rights and competition

Finding the right balance between protecting trademark rights and promoting fair competition is a complex issue. While a trademark is crucial for market distinctiveness and consumer protection excessive protection stifles innovation and limits consumer choices. Antitrust law here plays a very vital role in ensuring that the trademark law does not become the basis for the monopolization of power or the means of unfair practices. Antitrust regulators scrutinize the use of trademarks to prevent practices that hinder market entry or restrict the competition for new businesses. They evaluate situations where a dominant brand might use its trademark to suppress competitors or maintain unfair advantages. The new amendment bill which was called as competition (amendment) bill, 2020 was passed there are 2 major points are- the ambit of section 3(4) of the competition act, 2002 was expanded and it also includes the instances where the dominant positions in the ipr safe harbor. Here, this bill was passed to expand the limit of anti-competitive agreements. The clause is made in section 3(4) by the word 'any other agreement'. The second provision which deals with the ipr safe harbor was to work as security to intermediaries against any of the liability done by the third-party activities. The section 4a also came into existence to protect the intellectual property right holders and to strengthen their rights of ip.

Here, with the new development in the commercial environment, there was a connection created between the trademark and the competition law. Here, the trademark deals with the exclusive rights given to the owner over their innovation regarding their trademark mark, and trade secrets. The

LegalOnus Law Journal (LLJ)

competition law deals with protecting the market from the anti- competition to ensure the consumer gets a choice to differentiate the goods and services for the availing of the perfect products. The feature of distinctiveness in the trademark is provided to prevent the same use of the mark. So, together these laws work to ensure fair competition would be done without any unfair practices.

The trademark rights are issued for the protection of brand identity, by allowing the business to maintain and build consumer trust over such brand name. They prevent other businesses from the using same mark so that confusion could be created in the mind of consumers. Competition law aims to maintain a fair open market by eliminating monopolistic practices and anti-competitive exercises by encouraging innovation and more consumer choices. Also, the strong trademark creates a problem for the market, it creates market power for the popular brands. This can lead to limit the competition in the market if the brands use their trademark to stifle the rivals from the market, it limits the choices for the consumer.

The court often tried to use some doctrines like "fair use and the exhaustion" the limit the extent of the trademark protection, they tried to balance the rights of the trademark protection for the public interest. Fair use permits the other business to utilize the brand name to portray the products regardless of identical marks. Exhaustion restricts a brand name owner's control after the item is sold out, permitting the resale in the secondary markets, and advancing competition.

Also, in some specific cases, trademark licensing and organizations can raise antitrust concerns. Antitrust authorities might intervene if the company trademark strategy leads to the disregard of market competition or limits innovations. For, these things the trademark and competition law must have to work together. For, this the authorities of the trademark and competition law to work with each other in coordination to maintain the market economy and should work to safeguard the rights of the brand holders by supporting innovation consumer trust, and a fair market. A review was done to maintain the market and to prevent it from unfair practices. And by ensuring fair competition and preventing monopolization.

LegalOnus Law Journal (LLJ)

Conclusion and suggestions:

According to Daniel j. Boorstein: an image is more than just a design, phrase, logo, or picture that people can quickly recall. It is a carefully constructed personality profile of a person, organization, business, commodity, or service.

Each mark signifies and embodies an independent identity that must be kept and safeguarded. By combining the brand's ideals, reputation, and customer trust, trademarks help to shape the brand identity. Trademarks ensure market exclusivity and customer trust while offering legal protection against infringement and unauthorized use through registration and enforcement. While a trademark grants a right, competition law establishes a regulatory body that sets standards for the manufacture, distribution, storage, and supply of goods as well as the obligations placed on businesses operating in the market. It gives the author of a script or the developer of an inventive product the right to use it exclusively for a predetermined amount of time. To promote consumer welfare, goodwill, innovation, and economic growth, trademarks must be managed and protected effectively.

Trademark-enabled branding tactics, however, may also have antitrust ramifications. Trademarks can occasionally be exploited to establish or preserve market power, which may result in anti-competitive behavior, even if its primary purpose is to safeguard brand identity and encourage fair competition. For example, excessively strong or wide trademark enforcement can hinder innovation and competition, making it harder for new firms to enter the market and limiting the options available to consumers.

Policymakers should maintain a balance between protecting legitimate trademark rights and preventing abuse to restrict competition. Clear and not excessively broad trademark laws can help achieve this. Regulatory bodies should actively monitor the market for anti-competitive practices related to trademarks, including mergers and acquisitions that may consolidate market power. Promoting innovation can encourage a competitive environment where small businesses and startups can develop and protect their trademarks without facing legal challenges. Increase public awareness about the importance of trademarks and the potential for anti-competitive behavior.

LegalOnus Law Journal (LLJ)

Educating consumers about their rights and recognizing anti-competitive practices can mitigate negative impacts on the market. Regularly reviewing and updating trademark laws to keep pace with market changes and technological advancements ensures fair competition and protection of intellectual property rights. Implementing these suggestions can maximize the positive impact of trademarks on market distinctiveness while minimizing antitrust risks, and fostering a competitive and dynamic market environment.

References: -

- Trademark act, 1999 (act no. 47 of 1999)
- Avtar Singh and dr. Harpreet Kaur, competition law (eastern book company)
- S.r. Myneni, intellectual property rights in information technology (new era law publication)
- V.k. Ahuja, law relating to intellectual property rights (lexis nexis third edition)
- <https://www.drishtias.com/to-the-points/paper3/intellectual-property-rights>
- <https://blog.iplayers.in/concept-of-property/>
- <https://www.wipo.int/about-ip/en/>
- <https://www.indiafilings.com/learn/types-of-trademark/>
- <https://www.legalserviceindia.com/legal/article-16344-how-trademark-law-evolved-in-india-.html>
- <https://www.altacit.com/trademark/evolution-of-trademark-laws-in-india/>
- <https://ijrpr.com/uploads/v4issue9/ijrpr17505.pdf>

LegalOnus Law Journal (LLJ)

Recent Trends in Cybercrime and Data Protection Law

By

Aman Kumar Choudhary,

Co-author:

Shamsh s. Ahsan

Sweety kumari

Legalonus

LegalOnus Law Journal (LLJ)

Abstract:

The rapid evolution of technology has brought about unprecedented changes in the digital landscape, leading to significant advancements in communication, commerce, and data sharing. However, this digital revolution has also given rise to new challenges, particularly in the realm of cybercrime and data protection. This paper examines recent trends in cybercrime, such as ransomware attacks, data breaches, identity theft, and the growing threat of artificial intelligence in facilitating cyberattacks. It also explores the increasing role of social engineering techniques that exploit human psychology to compromise sensitive information.

On the legislative front, the study analyses the latest developments in data protection laws across various jurisdictions, focusing on landmark regulations such as the general data protection regulation (gdpr) in europe, the California consumer privacy act (ccpa) in the united states, and emerging frameworks in other regions. The paper highlights the growing trend towards stricter data protection standards, the emphasis on user consent, and the challenges posed by cross-border data transfers.

Furthermore, the paper discusses the evolving relationship between technology companies, law enforcement agencies, and regulators, particularly in the context of data protection and privacy rights. By examining these trends, this study aims to provide a comprehensive understanding of the dynamic and evolving nature of cybercrime and data protection laws, offering insights into how legal frameworks can adapt to the ever-changing cyber landscape.

Keywords: cybercrime, data protection law, privacy, artificial intelligence, social engineering, cybersecurity trends, cross-border data transfers

1.introduction

The digital age has transformed the way individuals, businesses, and governments operate, ushering in an era of unparalleled connectivity and data-driven innovation. However, alongside

LegalOnus Law Journal (LLJ)

the benefits of digitization, the rise of cybercrime has become a pressing concern. As more data is stored, processed, and transmitted online, the risk of cyberattacks and unauthorized data access has increased exponentially. This has prompted governments, organizations, and regulatory bodies around the world to implement robust legal frameworks aimed at combating cybercrime and protecting sensitive data. In this context, understanding the recent trends in cybercrime and the development of data protection laws is critical for creating a safer digital environment.

1.1. Background and context

Cybercrime, which encompasses a wide range of illegal activities carried out through the internet or involving digital technology, has grown in both scope and sophistication. From phishing scams and identity theft to large-scale data breaches and ransomware attacks, cyber threats are evolving at an alarming rate. Meanwhile, data protection laws have also gained prominence in response to the increasing volume of personal and financial data being shared and stored digitally. Landmark regulations such as the general data protection regulation (gdpr) in the European union and the California consumer privacy act (ccpa) in the united states have set new standards for data privacy and security.

This paper will explore the interplay between these two areas—cybercrime and data protection laws—by analysing recent trends and assessing how legal frameworks are evolving to address the threats posed by cybercriminals in a globalized, digitally connected world.

1.2. Importance of cybercrime and data protection

The importance of addressing cybercrime and enhancing data protection cannot be overstated. With digital systems now integral to critical sectors such as finance, healthcare, education, and national security, a single breach can lead to far-reaching consequences, including financial losses, reputational damage, and threats to national security. Furthermore, the widespread collection and processing of personal data by corporations and governments have raised concerns about privacy rights, leading to growing demand for stringent legal protections.

LegalOnus Law Journal (LLJ)

Data protection laws play a pivotal role in safeguarding individual privacy, ensuring transparency in data handling, and establishing accountability for entities that collect, store, and process personal information. At the same time, cybercrime legislation is essential for deterring and prosecuting individuals or groups involved in illegal cyber activities. The convergence of these legal areas is vital for maintaining trust in the digital economy.

1.3. Objectives of the study

The primary objective of this study is to examine the recent trends in cybercrime and how data protection laws are adapting to these challenges. Specifically, the study aims to:

- Analyse the current landscape of cybercrime, including emerging threats such as ransomware, artificial intelligence-driven attacks, and identity theft.
- Investigate the evolution of global data protection frameworks, focusing on key regulations like gdpr, ccpa, and other regional laws.
- Identify the challenges and opportunities in aligning cybercrime prevention measures with data protection laws.
- Provide recommendations for policymakers and stakeholders on how to strengthen legal responses to cyber threats and improve data protection standards.

1.4. Structure of the paper

This paper is structured into several sections to provide a comprehensive analysis of the subject matter. The next section (section 2) provides an in-depth examination of cybercrime, including definitions, key types of cyberattacks, and recent trends in this area. Section 3 focuses on data protection laws, covering the key legal frameworks that govern data privacy and security

LegalOnus Law Journal (LLJ)

worldwide. Section 4 explores the intersection of cybercrime and data protection, highlighting the legal and technological challenges that arise in this context.

Section 5 presents case studies and key legal precedents, offering real-world examples of how cybercrime and data protection laws are applied. Section 6 identifies gaps and challenges in existing legislation and provides a critical analysis of emerging technologies and their legal implications. Finally, section 7 outlines future directions for policy and legislative reforms, and section 8 concludes the paper with a summary of key findings and recommendations.

2. Understanding cybercrime

2.1. Definition and types of cybercrime

Cybercrime refers to criminal activities carried out using computers or the internet. These crimes range from attacks on systems, networks, and data to illicit activities conducted through digital channels. Broadly, cybercrimes can be categorized into two types: crimes that target computers (e.g., hacking, malware, and denial-of-service attacks) and crimes that use computers as a tool to facilitate traditional offenses (e.g., identity theft, fraud, and child exploitation). As technology continues to evolve, the scope of cybercrime expands, posing increasingly complex challenges for legal systems, law enforcement, and cybersecurity professionals.

2.2. Recent trends in cybercrime

The rise in cybercrime in recent years has seen the emergence of new techniques and an increase in the sophistication of attacks. Below are some of the most significant trends shaping the cybercrime landscape today:

2.2.1. Ransomware and malware attacks

Ransomware is one of the fastest-growing forms of cybercrime, where attackers use malware to encrypt a victim's data and demand payment, typically in cryptocurrency, for its release. High-profile attacks on organizations, government bodies, and critical infrastructure have highlighted the devastating impact of ransomware, which can lead to massive financial losses, operational

LegalOnus Law Journal (LLJ)

disruptions, and reputational damage. Malware, in various forms such as viruses, worms, and trojans, continues to be a significant threat to personal and corporate data security.

2.2.2. Phishing and social engineering

Phishing involves fraudulent attempts to obtain sensitive information such as usernames, passwords, and credit card details by impersonating trustworthy entities in electronic communications. Social engineering exploits human psychology to trick individuals into disclosing confidential information. These techniques remain prevalent due to their low cost and high success rates, often bypassing technological defences by targeting human error.

2.2.3. Identity theft and financial fraud

Identity theft involves the unauthorized use of personal information to commit fraud, such as opening accounts, making purchases, or obtaining credit under someone else's name. With increasing amounts of personal data stored and shared online, identity theft has become a pervasive issue. Financial fraud, ranging from credit card fraud to online banking attacks, has also surged, with cybercriminals targeting digital financial systems and platforms.

2.2.4. Role of artificial intelligence in cyberattacks

Artificial intelligence (ai) is being increasingly leveraged by cybercriminals to enhance the efficiency, scale, and sophistication of their attacks. Ai can automate tasks such as scanning for vulnerabilities, executing phishing campaigns, and deploying malware. More concerning is the potential for ai-driven autonomous cyberattacks, where machine learning algorithms could make decisions without human input, posing a new kind of threat to cybersecurity.

2.3. Key global cybercrime statistics

Cybercrime is now a global issue, with both developed and developing nations facing its impacts. According to recent reports, the global cost of cybercrime is estimated to reach over \$10.5 trillion annually by 2025, making it more profitable than the global drug trade. In 2023 alone, ransomware attacks accounted for more than 25% of all cyberattacks, with healthcare, finance, and education

LegalOnus Law Journal (LLJ)

sectors being the hardest hit. Phishing remains the top method of cyberattack, with over 90% of data breaches attributed to phishing campaigns. Moreover, as global digital connectivity increases, emerging markets are becoming increasingly targeted by cybercriminals, underlining the need for international cooperation in combatting these offenses.

3. Data protection laws: an overview

Data protection laws have become an essential aspect of modern governance, particularly in an era where personal information is collected, processed, and shared on a massive scale by both private and public entities. As digital transactions and interactions continue to grow, so does the need for robust legal frameworks to protect individuals' privacy and personal data. This section provides an in-depth overview of key global data protection frameworks, their common features, and their impact on businesses and individuals.

3.1. Global data protection frameworks

The rise of privacy concerns globally has prompted various countries to establish comprehensive data protection laws. While the core purpose of these laws is to protect individuals' data privacy, the specific requirements and enforcement mechanisms vary by jurisdiction. This subsection explores prominent data protection frameworks, including the European union's general data protection regulation (gdpr), the united states' California consumer privacy act (ccpa), and emerging frameworks in other regions.

3.1.1. The European union's gdpr

The general data protection regulation (gdpr), implemented in May 2018, is one of the most stringent and far-reaching data protection laws globally. It applies not only to companies operating within the European union (EU) but also to those outside the EU that handle the personal data of EU citizens. The gdpr is built around key principles like transparency, data minimization, and accountability, emphasizing the protection of individual rights regarding their data. Some of the key provisions of the gdpr include:

LegalOnus Law Journal (LLJ)

- Data subject rights: the gdpr grants individuals a range of rights, including the right to access their data, the right to rectification, the right to erasure (also known as the “right to be forgotten”), and the right to data portability.
- Consent: under the gdpr, data controllers must obtain explicit consent from individuals before collecting and processing their data. This consent must be freely given, informed, and revocable.
- Accountability and governance: companies are required to implement data protection measures, appoint data protection officers (dpos) in some cases, and ensure data processing activities are documented.
- Breach notification: the regulation mandates that data breaches be reported to the relevant authority within 72 hours, and individuals must be informed if the breach poses a significant risk to their rights and freedoms.
- Cross-border data transfers: the gdpr restricts the transfer of personal data outside the EU unless adequate data protection standards are in place.

The gdpr is lauded for its stringent fines, with penalties of up to 4% of a company's global annual revenue or €20 million, whichever is higher, for non-compliance.

3.1.2. The united states' ccpa and other federal laws

In contrast to the gdpr, the united states lacks a single, unified federal data protection law. Instead, it has a patchwork of state-level regulations, with the California consumer privacy act (ccpa) being the most notable. Enacted in 2020, the ccpa grants California residents new rights concerning the collection and sale of their personal data. Key aspects of the ccpa include:

LegalOnus Law Journal (LLJ)

- Right to access and deletion: similar to the gdpr, the ccpa allows individuals to request access to the personal data that businesses have collected about them, as well as the right to request deletion.
- Opt-out of data sale: one of the unique features of the ccpa is the right for consumers to opt out of the sale of their personal data to third parties. Businesses must include a "do not sell my personal information" link on their websites.
- Transparency: businesses are required to inform consumers at the time of data collection about the categories of personal data being collected and the purposes for which they will be used.
- Limited applicability: the ccpa applies to businesses that meet certain thresholds, such as annual gross revenues above \$25 million, handling personal data of 50,000 or more consumers, or deriving 50% or more of annual revenues from selling personal information.

While the ccpa is one of the most comprehensive state-level privacy laws, there are other laws, such as the children's online privacy protection act (coppa) and the health insurance portability and accountability act (hipaa), which protect specific categories of data in the u.s.

3.1.3. Data protection initiatives in other jurisdictions

Outside the EU and the u.s., many other countries have enacted or are in the process of enacting data protection laws that reflect elements of the gdpr or ccpa:

- Brazil: the lei geral de proteção de dados (lgpd) came into effect in 2020 and mirrors many of the gdpr's principles, including consent, data subject rights, and breach notification requirements.
- India: India's personal data protection bill, currently in the legislative process, seeks to introduce strict data protection norms, drawing inspiration from the gdpr. However, it also includes government access provisions that have sparked debates over privacy.

LegalOnus Law Journal (LLJ)

- Australia: Australia's privacy act 1988, while not as comprehensive as the gdpr, contains important rules on how personal data can be collected, used, and disclosed.
- Japan: Japan's act on the protection of personal information (appi) was amended in 2020 to strengthen individual rights and impose stricter data breach reporting obligations.

These global frameworks highlight the increasing trend towards robust data protection laws, although the specifics of enforcement and compliance vary.

3.2. Common features and legal obligations

Despite regional variations in data protection laws, certain core principles and obligations are consistently present across frameworks. These common features form the foundation for regulating personal data processing:

- Consent and transparency: most data protection laws require clear and explicit consent from individuals before collecting or processing their data. Companies must also be transparent about how data will be used, shared, and stored.
- Data minimization: organizations are generally required to collect only the data that is necessary for the specific purpose identified at the time of collection.
- Data subject rights: individuals are commonly granted rights such as access to their data, the ability to correct inaccuracies, the right to deletion, and the ability to object to certain types of data processing.
- Accountability and governance: laws require organizations to implement appropriate technical and organizational measures to safeguard personal data. This may include appointing a data protection officer (dpo) and conducting impact assessments for high-risk processing activities.
- Data breach notification: prompt reporting of data breaches is a universal requirement, with specific timelines for notification set by the respective regulations.

LegalOnus Law Journal (LLJ)

- Cross-border data transfers: laws typically restrict the transfer of personal data to countries without adequate data protection standards unless additional safeguards, such as standard contractual clauses, are in place.

3.3. Impact of data protection laws on business and individuals

Data protection laws have a profound impact on both businesses and individuals:

- For businesses: compliance with data protection laws often requires significant investment in data security infrastructure, legal compliance programs, and employee training. Companies face hefty fines for non-compliance, which can lead to reputational damage. Additionally, businesses must navigate the complexities of international data transfers, especially in industries with a global footprint, such as technology and e-commerce. On the positive side, complying with stringent data protection laws can increase consumer trust and loyalty.
- For individuals: data protection laws empower individuals by giving them control over their personal information. They can access, correct, and even delete their data, which enhances privacy and security. However, individuals must also be proactive in exercising their rights and understanding how their data is being used by organizations. Enhanced legal protections contribute to safeguarding individuals from identity theft, fraud, and unauthorized data exploitation.

4. The intersection of cybercrime and data protection

The relationship between cybercrime and data protection is deeply interconnected. In today's digital age, data is one of the most valuable commodities, making it a prime target for cybercriminals. The rise in cybercrime, particularly attacks on personal and sensitive data, highlights the urgent need for robust data protection frameworks. This section explores key points where cybercrime and data protection laws intersect, focusing on data breaches, cross-border data transfer challenges, technological safeguards like encryption and cloud security, and legal responses to cybercrime targeting personal data.

LegalOnus Law Journal (LLJ)

4.1. Data breaches: a key nexus

Data breaches represent one of the most significant intersections between cybercrime and data protection. When cybercriminals gain unauthorized access to data, they often exploit it for financial gain, identity theft, or corporate espionage. The scale of these breaches has grown exponentially in recent years, affecting millions of individuals and corporations worldwide.

Data breaches occur through various means, including hacking, malware, phishing, and insider threats. High-profile incidents, such as the breaches of Equifax, yahoo, and Marriott international, exposed the personal information of millions, highlighting the vulnerabilities in corporate data security practices.

From a legal perspective, data protection laws like the general data protection regulation (gdpr) and the California consumer privacy act (ccpa) impose strict obligations on organizations to safeguard personal data. These laws require organizations to implement technical and organizational measures to prevent data breaches and mandate that breaches be reported to regulatory authorities within a specific timeframe. Failure to protect data adequately or to report breaches in a timely manner can result in substantial penalties, as seen with fines levied against major corporations under gdpr provisions.

Thus, data breaches exemplify the convergence of cybercrime and the legal frameworks designed to protect individuals' data. As cybercriminals continue to exploit vulnerabilities in systems, data protection laws must evolve to address new threats and better protect sensitive information.

4.2. Cross-border data transfer challenges

The global nature of the internet and digital commerce has made cross-border data transfers an essential part of international business. However, transferring data across borders introduces

LegalOnus Law Journal (LLJ)

complex legal and security challenges, especially as countries enact different data protection regulations.

One of the primary challenges in cross-border data transfers is ensuring compliance with diverse legal frameworks. For instance, the gdpr in the European union places strict restrictions on transferring personal data to countries outside the EU that do not offer adequate levels of data protection. This has led to the development of standard contractual clauses (scs) and binding corporate rules (bcrs) as mechanisms to facilitate legal data transfers while ensuring compliance with the gdpr's high standards.

At the same time, countries like the united states have adopted more lenient approaches to data privacy, leading to legal clashes over data transfers. The Schrems ii ruling by the European court of justice, which invalidated the EU-u.s. Privacy shield framework, demonstrated the tension between European data protection standards and u.s. Surveillance practices.

Cross-border data transfers also pose security risks. Cybercriminals often exploit differences in data protection laws between jurisdictions to target data being transferred across international borders. The lack of harmonized data protection laws creates vulnerabilities that criminals can leverage. Consequently, organizations must invest heavily in securing data during transit and at rest, employing technologies such as end-to-end encryption and secure data transfer protocols to mitigate risks.

4.3. Role of technology in securing data

In the battle against cybercrime, technology plays a crucial role in protecting personal and corporate data. As cyber threats become more sophisticated, organizations are increasingly turning to advanced security measures to safeguard sensitive information and comply with data protection regulations.

4.3.1. Encryption

LegalOnus Law Journal (LLJ)

Encryption is one of the most effective tools in protecting data from unauthorized access. It works by converting data into a format that is unreadable without a decryption key, ensuring that even if cybercriminals intercept or steal the data, they cannot use it without the appropriate credentials.

Data protection laws such as gdpr explicitly encourage encryption as a means of securing personal data. Under article 32, gdpr mandates that organizations implement "appropriate technical and organizational measures," with encryption being specifically mentioned as a recommended method for safeguarding data.

There are two primary types of encryption: in-transit encryption and at-rest encryption. In-transit encryption protects data as it moves across networks (such as during an online transaction), while at-rest encryption secures data stored on servers or devices. The implementation of both forms of encryption helps reduce the risk of data breaches and meets legal requirements for protecting personal data.

However, encryption presents its own set of challenges, particularly in balancing privacy and law enforcement needs. Governments often seek backdoor access to encrypted communications for national security reasons, which raises concerns about undermining privacy protections.

4.3.2. Cloud security

As more organizations adopt cloud computing services, cloud security has become a central concern in data protection efforts. Cloud services offer significant advantages in terms of scalability, cost savings, and accessibility, but they also introduce new risks related to data privacy and security.

Cloud environments are attractive targets for cybercriminals due to the large volumes of sensitive data they hold. Misconfigurations, insecure apis, and inadequate access controls are common vulnerabilities that criminals exploit in cloud infrastructure. High-profile cloud-related breaches, such as the capital one breach, have underscored the importance of securing cloud environments.

LegalOnus Law Journal (LLJ)

To address these risks, organizations must adopt comprehensive cloud security strategies, which include encryption of data stored in the cloud, multi-factor authentication, and regular security audits. Cloud providers, too, are subject to legal obligations under data protection laws. For example, under gdpr, cloud providers act as “data processors” and must ensure that appropriate security measures are in place to protect personal data processed on behalf of their clients.

4.4. Legal responses to cybercrime targeting personal data

Governments and regulatory bodies worldwide have responded to the growing threat of cybercrime targeting personal data by enacting stringent data protection and cybersecurity laws. These laws aim to create a legal framework that holds organizations accountable for safeguarding personal data while providing enforcement mechanisms to combat cybercrime.

Key legislative responses include:

- General data protection regulation (gdpr): one of the most comprehensive data protection laws globally, the gdpr sets strict guidelines for how organizations collect, process, and store personal data. It also includes provisions for handling data breaches, mandating that organizations notify authorities and affected individuals within 72 hours of a breach.
- California consumer privacy act (ccpa): in the united states, the ccpa provides California residents with specific rights over their personal data, including the right to know what data is collected, the right to request deletion, and the right to opt out of data sales. The ccpa also imposes obligations on businesses to secure personal data and includes penalties for data breaches.
- Cybercrime legislation: in addition to data protection laws, many jurisdictions have enacted specific cybercrime laws. These laws address offenses such as hacking, identity theft, and unauthorized access to data. For instance, the computer fraud and abuse act (cfaa) in the u.s. Criminalizes various forms of cybercrime, including unauthorized access to computers and networks.

LegalOnus Law Journal (LLJ)

Despite these legal frameworks, challenges remain. The rapid pace of technological innovation often outstrips the ability of lawmakers to keep up, creating gaps in regulation. Moreover, the international nature of cybercrime complicates enforcement, as cybercriminals often operate across borders, exploiting differences in legal systems.

5. Case studies and key legal precedents

5.1. Landmark cybercrime cases (Indian cases)

India has witnessed a significant rise in cybercrime over the past decade, prompting various landmark cases that have shaped the legal landscape. Some of the most notable cases include:

1. The pune citibank mphasis call center fraud (2005):

This was one of the earliest high-profile cybercrime cases in India, where employees of a BPO (business process outsourcing) associated with Citibank illegally accessed confidential customer accounts and siphoned off approximately ₹1.5 crores. The case highlighted the vulnerability of sensitive data in outsourcing industries and marked a turning point for India's cybercrime regulations, resulting in stricter oversight of data access protocols and outsourcing operations.

2. The Sony sambandh case (2004):

One of the first cyber defamation cases, this case involved a dispute between an individual and a company, Sony India Private Ltd. A man purchased a product through Sony's website, but the product was not delivered, leading to a complaint. When he didn't receive the response he wanted, he created defamatory content online about Sony. The case was significant because it established the idea of internet defamation within Indian cyber laws and led to judicial recognition of the Information Technology (IT) Act, 2000, as covering cyber defamation.

3. The bank nsp case (2001):

LegalOnus Law Journal (LLJ)

In this case, an employee of bank nsp (a pseudonym for privacy purposes) was found guilty of manipulating his fiancé's bank account and email information. He fraudulently transferred funds from her bank account and altered her online banking details. This case was critical because it was one of the earliest instances where Indian courts dealt with online banking fraud and identity theft. It underscored the need for comprehensive legislation on cybercrimes, specifically related to financial data protection and identity fraud.

4. The emoted malware attack (2021):

This more recent case involved the sophisticated emotet malware, which affected several Indian government organizations. The attack primarily focused on stealing financial data, leading to a nationwide alert issued by the Indian computer emergency response team (cert-in). The case emphasized the growing threat of advanced malware attacks in india and highlighted the importance of enhancing cybersecurity measures within government agencies and critical infrastructures.

5. The Arogya Setu data leak controversy (2020):

The Arogya Setu app, designed to trace covid-19 cases, was embroiled in a controversy when it was reported that personal data of millions of users was vulnerable to leaks. Ethical hackers raised concerns over the privacy and security protocols of the app, which led to widespread debate about the government's role in data protection. Although no significant breach was confirmed, the controversy highlighted gaps in data protection in government-deployed applications and sparked the urgent need for a stronger personal data protection framework in india.

5.2. Notable data protection lawsuits

1. Justice k.s. Puttaswamy v. Union of india (2017):

This landmark case, commonly referred to as the Aadhaar case, was a pivotal moment in Indian jurisprudence regarding the right to privacy. The supreme court ruled that the right to privacy is a fundamental right under article 21 of the Indian constitution. The case emerged from concerns

LegalOnus Law Journal (LLJ)

surrounding the Aadhaar system, a massive biometric database used for identifying Indian citizens. Petitioners argued that the government's collection and storage of personal information without adequate safeguards violated privacy rights. Although the court upheld the validity of the Aadhaar scheme, it mandated several restrictions to protect individual privacy. This ruling laid the foundation for India's future data protection laws, influencing the drafting of the personal data protection bill.

2. Facebook india online services pvt. Ltd. V. Ajit Mohan & ors (2020):

This case revolved around the Delhi legislative assembly's summons issued to Facebook regarding the platform's alleged role in spreading misinformation and inciting violence during the Delhi riots. Facebook argued that the proceedings violated its rights, especially concerning data privacy and intermediary liability. The supreme court held that the platform had to cooperate with law enforcement, but it raised important questions about the responsibilities of social media platforms in managing data and misinformation under India's legal framework.

3. Anivar aravind v. Union of india (2020):

Another notable case involving the Arogya Setu app, where the petitioner challenged the mandatory use of the app, arguing that it violated privacy rights and data protection principles, especially because no formal data protection law had been enacted in india at the time. While the supreme court did not pass a decisive ruling against the app, it led to further discourse on voluntary versus mandatory use of data-collecting applications and emphasized the need for legislative clarity on data protection and privacy.

4. WhatsApp privacy policy case (2021):

In this case, concerns were raised about WhatsApp's updated privacy policy, which allowed the platform to share users' data with its parent company, Facebook, and other third-party entities. The matter was brought before the Delhi high court, with petitioners arguing that the policy violated privacy rights and lacked sufficient transparency. The case gained global attention and led to

LegalOnus Law Journal (LLJ)

increased scrutiny of tech giants in india, adding urgency to the enactment of the personal data protection bill.

5.3. Analysis of global regulatory responses

1. The European union's general data protection regulation (gdpr): the gdpr, implemented in May 2018, represents one of the most comprehensive data protection laws globally. It sets a high standard for data protection, emphasizing user consent, transparency, and accountability. It also establishes strict regulations for cross-border data transfers and imposes heavy penalties for non-compliance. The gdpr has influenced data protection laws in other regions, including India's pending personal data protection bill, which draws upon its principles. The gdpr has also led to multinational corporations revising their data handling practices to ensure compliance, highlighting the global ripple effect of regional legislation.

2. California consumer privacy act (ccpa):

The ccpa, which came into effect in January 2020, is another key development in the global data protection landscape. Focused on enhancing the privacy rights of California residents, it mandates that businesses disclose what data they collect and how it is used, while also allowing consumers to opt out of data collection. While the ccpa is state-specific, its influence extends beyond California due to the global reach of tech companies headquartered in the state. It represents a growing trend in the u.s. Toward more robust data protection laws, challenging the country's traditionally fragmented approach to privacy.

3. Brazil's general data protection law (lgpd):

Brazil's lgpd, which came into effect in September 2020, is similar to the gdpr in many respects, emphasizing the protection of personal data and providing users with control over their data. The law applies to any business that processes personal data in Brazil, making it part of the global trend of strengthening data privacy regulations. Lgpd's extraterritorial application, much like the gdpr, underscores the need for global businesses to be mindful of data protection across multiple jurisdictions.

LegalOnus Law Journal (LLJ)

4. Indian personal data protection bill (pdpb):

India's personal data protection bill, first introduced in 2019, is heavily inspired by the gdpr and seeks to establish a comprehensive legal framework for data protection. While the bill is still under review, it outlines strict data processing obligations, recognizes the rights of data principals (individuals), and establishes a data protection authority (dpa). The pdpb represents India's attempt to balance the need for data-driven innovation with the protection of individual privacy. However, the bill has faced criticism for granting broad exemptions to government agencies, which raises concerns about the balance between state surveillance and individual rights.

5. Global harmonization and regulatory gaps:

While the gdpr sets a high bar for global data protection, there is still a lack of harmonization among global cybercrime and data protection regulations. Countries vary widely in their approaches, leading to challenges in cross-border enforcement and data transfer. The absence of a universal framework complicates efforts to combat global cybercrime effectively. The regulatory gaps are particularly apparent in regions where cybersecurity laws are either outdated or insufficient to address the complexities of modern cyberattacks.

6. Challenges and gaps in cybercrime and data protection legislation

Despite significant strides in addressing cybercrime and enhancing data protection through various legislative efforts, critical challenges and gaps remain. The rapidly evolving nature of technology continues to outpace legislative frameworks, leading to inconsistencies and loopholes that cybercriminals exploit. This section explores some of the most pressing challenges that governments and regulators face globally, focusing on the lack of harmonization in international cyber laws, regulatory gaps in emerging technologies, and the delicate balance between security, privacy, and innovation.

6.1. Lack of harmonization in global cyber laws

LegalOnus Law Journal (LLJ)

One of the most significant challenges in combating cybercrime is the absence of a unified international legal framework. Cybercrime, by its very nature, transcends national borders, with cybercriminals often operating in jurisdictions different from where their victims reside. The lack of harmonization between national cybercrime laws complicates efforts to investigate, prosecute, and convict cybercriminals. Different countries have varying definitions of cybercrime, different legal standards for evidence collection, and varying levels of enforcement.

For instance, the European union has adopted comprehensive data protection regulations like the general data protection regulation (gdpr), while the united states follows a sectoral approach with laws like the California consumer privacy act (ccpa). Countries in Asia and Africa are at different stages of developing and implementing cybercrime and data protection laws, creating a patchwork of regulations that make cross-border enforcement difficult.

This inconsistency poses several problems. First, cybercriminals can exploit jurisdictions with weaker laws to carry out attacks against targets in more regulated regions. Second, companies engaged in international business face the complexity of complying with multiple, sometimes conflicting, legal regimes, leading to increased operational costs. Third, victims of cybercrime may find it challenging to seek legal recourse when the perpetrators operate under different legal systems with little cooperation.

Efforts like the Budapest convention on cybercrime have aimed at promoting international cooperation, but its adoption remains limited, and many nations, including some major players like Russia and China, have opted out. Without greater harmonization, international law enforcement coordination will remain a significant hurdle in addressing global cybercrime.

6.2. Regulatory gaps in emerging technologies (ai, iot)

The rapid rise of emerging technologies such as artificial intelligence (ai), the internet of things (iot), and blockchain has introduced new vulnerabilities that current cybercrime and data protection laws have not adequately addressed. These technologies have transformed industries

LegalOnus Law Journal (LLJ)

and daily life, but they also create complex regulatory challenges due to their decentralized, interconnected, and rapidly evolving nature.

Artificial intelligence (ai): ai is increasingly used both by defenders and attackers in cybersecurity. Ai can help detect and prevent cyberattacks through machine learning algorithms that identify patterns and anomalies in data traffic. However, cybercriminals can also use ai to automate and scale attacks, such as using ai-driven bots for phishing attacks or deploying ai tools for more sophisticated hacking. The regulatory gap here lies in the lack of specific frameworks governing the ethical and responsible use of ai in both cybersecurity and data protection. Current laws are ill-equipped to handle ai's autonomous decision-making processes, raising concerns about accountability and liability when ai systems fail or are used maliciously.

Internet of things (iot): the iot ecosystem, encompassing billions of interconnected devices, is highly vulnerable to cyberattacks. Iot devices often lack robust security features, and their sheer number creates a vast attack surface for cybercriminals. Many existing regulations do not explicitly cover the security standards required for iot devices, leaving consumers exposed to risks such as data breaches, device hijacking, and large-scale distributed denial of service (ddos) attacks. Moreover, the fragmented nature of iot device manufacturers, who operate in different jurisdictions with varying levels of regulation, exacerbates the problem. Clear global standards for iot security, including mandatory encryption and regular security updates, are still in development.

Blockchain and cryptocurrencies: blockchain technology, while offering enhanced security for data integrity and transparency, also facilitates anonymity in transactions, making it a favoured tool for cybercriminals engaging in illicit activities like money laundering and ransomware payments. Existing financial regulations have struggled to adapt to the rise of cryptocurrencies, and there is still a lack of international consensus on how to regulate digital currencies in the context of cybercrime prevention and data protection.

LegalOnus Law Journal (LLJ)

Without comprehensive regulatory frameworks for these emerging technologies, the risk of cybercrime will continue to grow, exploiting these gaps to bypass traditional security and legal safeguards.

6.3. Balancing security, privacy, and innovation

A core challenge in developing effective cybercrime and data protection laws is finding a balance between ensuring security, protecting individual privacy, and fostering innovation. Each of these elements is crucial, but they often come into conflict with one another.

Security vs. Privacy: governments and law enforcement agencies argue that to protect national security and combat cybercrime, they need access to personal data, including encrypted communications. However, this poses a significant threat to individual privacy rights. For example, the debate around encryption "backdoors" exemplifies this tension. While backdoors could enable authorities to access encrypted data in criminal investigations, they could also weaken the overall security of digital systems, making them more vulnerable to cyberattacks.

Furthermore, surveillance measures like mass data collection programs, which are sometimes justified on the grounds of national security, often conflict with data protection laws such as the gdpr, which emphasizes user consent and the right to privacy. Striking the right balance between empowering law enforcement and protecting individual privacy remains a contentious issue.

Privacy vs. Innovation: innovation in fields like ai, data analytics, and iot often depends on the collection and processing of vast amounts of data, raising privacy concerns. Data protection laws that are too stringent could stifle innovation by restricting the free flow of information and adding regulatory burdens on companies. For instance, startups developing new technologies may struggle with compliance costs, while large multinational corporations may navigate the regulations more easily.

Security vs. Innovation: on the other hand, focusing too heavily on security can slow down technological advancement. Overregulation in cybersecurity might discourage companies from adopting new technologies due to concerns about legal liabilities. For example, firms might

LegalOnus Law Journal (LLJ)

hesitate to implement ai-driven solutions if the legal environment holds them strictly accountable for any errors or vulnerabilities in the system.

The challenge for lawmakers is to create flexible yet robust regulations that can adapt to the rapid pace of technological change while protecting the fundamental rights of individuals. Policies must be crafted in a way that they do not hinder technological advancement but ensure that innovations are implemented responsibly and securely.

7. Future directions in cybercrime prevention and data protection

The increasing scale, complexity, and global nature of cybercrime have made it imperative for governments, organizations, and individuals to evolve and adapt to new threats. As both cybercrime and data protection challenges become more intertwined, proactive strategies are necessary to safeguard personal data and sensitive information. This section discusses key future directions that can significantly shape the landscape of cybercrime prevention and data protection.

7.1. Strengthening international cooperation

Cybercrime often transcends national borders, with perpetrators exploiting the global nature of the internet to carry out attacks from remote locations. This borderless aspect of cybercrime presents significant challenges for law enforcement agencies, as legal frameworks, resources, and capabilities vary widely across countries. To effectively combat this growing threat, enhanced international cooperation is essential. This can take multiple forms:

- **Multilateral agreements and treaties:** international treaties like the Budapest convention on cybercrime, adopted by the council of europe, have laid the foundation for international cooperation in addressing cybercrime. However, expanding participation in such agreements and creating new treaties tailored to emerging cyber threats is crucial. These agreements should facilitate cross-border investigations, evidence sharing, and the

LegalOnus Law Journal (LLJ)

extradition of cybercriminals while ensuring data protection and privacy rights are maintained.

- Joint cybersecurity task forces: international cybercrime task forces can be strengthened to promote better information sharing, joint operations, and coordinated responses to cyberattacks. Agencies such as Interpol and Europol have played important roles in facilitating such efforts, but more robust collaboration with regional organizations and private sector partners is needed to keep pace with rapidly evolving threats.
- Harmonizing cybercrime legislation: one of the main obstacles to international cooperation is the discrepancy in cybercrime laws across jurisdictions. Harmonizing cybercrime legislation can help standardize definitions of offenses, punishments, and investigative procedures. This will ensure that cybercriminals cannot exploit legal loopholes by operating in countries with weaker enforcement regimes.

7.2. Emerging legal and regulatory trends

As cyber threats evolve, the legal and regulatory frameworks that govern data protection and cybersecurity must also adapt to ensure adequate protection for individuals and organizations. The following trends are expected to shape the future of cybercrime prevention and data protection law:

- Stricter data protection regulations: the success of the EU's general data protection regulation (gdpr) has set a global standard for data protection, influencing countries to adopt similar frameworks. The California consumer privacy act (ccpa) and its updates, along with Brazil's lei geral de proteção de dados (lgpd), reflect a growing global movement towards comprehensive data privacy laws. Moving forward, more countries are expected to introduce stringent regulations, particularly regarding user consent, data minimization, and the right to be forgotten. This will place greater accountability on companies to protect personal data and provide transparent data processing practices.

LegalOnus Law Journal (LLJ)

- Increased regulation of emerging technologies: as technologies like artificial intelligence (ai), the internet of things (iot), and blockchain become more prevalent, new regulatory frameworks will be necessary to address their unique security risks. Ai, in particular, presents challenges in terms of its potential misuse for cyberattacks, while iot devices often lack robust security measures, making them vulnerable to exploitation. Governments are expected to introduce specific regulations mandating stronger security protocols for these technologies, requiring built-in security by design and more stringent certification standards.
- Cross-border data transfer regulations: with increasing reliance on global cloud services and data processing across jurisdictions, the regulation of cross-border data flows is becoming a critical issue. While frameworks like the EU-u.s. Data privacy framework and standard contractual clauses provide mechanisms for legal data transfers, the future may see more robust requirements, especially concerning third-country transfers. Ensuring adequate levels of protection for personal data in non-EU countries will likely become more challenging, with regulators potentially introducing stricter transfer mechanisms or regional data storage mandates.

7.3. The role of public awareness and education

While robust legal frameworks and international cooperation are vital for combatting cybercrime, raising public awareness and fostering a culture of cybersecurity are equally important. As human error remains one of the most exploited vulnerabilities in cyberattacks, educating the public can significantly reduce the success rate of attacks like phishing, social engineering, and ransomware.

- Promoting cyber hygiene: governments, businesses, and educational institutions should prioritize cybersecurity awareness campaigns that teach individuals the importance of basic security practices, such as using strong passwords, enabling multi-factor authentication, recognizing phishing attempts, and securing personal devices. Simple measures can dramatically reduce the likelihood of falling victim to cybercrime.

LegalOnus Law Journal (LLJ)

- Incorporating cybersecurity into educational curricula: to foster long-term resilience against cyber threats, cybersecurity should be integrated into school curricula at both primary and secondary levels. Teaching students the fundamentals of online safety, data protection, and digital ethics will ensure that future generations are better equipped to navigate the internet securely. Additionally, universities and vocational training institutions should expand their offerings in cybersecurity and data protection courses to address the growing demand for professionals in this field.
- Collaborating with the private sector: many cybercrime prevention initiatives will require close collaboration with the private sector, especially technology companies. These firms are often at the frontlines of detecting and responding to cyber threats. Public-private partnerships can facilitate the sharing of threat intelligence and best practices, while also encouraging technology companies to implement user-friendly security measures in their products and services.
- Cybersecurity certification and training for the workforce: given the increasing reliance on digital tools and platforms in the workplace, there is a growing need for employee training in cybersecurity practices. Organizations should implement regular cybersecurity training sessions, covering topics such as recognizing suspicious emails, safeguarding sensitive data, and responding to potential breaches. Additionally, industries may see the emergence of mandatory cybersecurity certifications for certain roles, particularly in sectors like finance, healthcare, and critical infrastructure.

Legalonus

LegalOnus Law Journal (LLJ)

Conclusion

8.1. Summary of key findings

This study has demonstrated that the exponential growth of technology and the increasing reliance on digital platforms have drastically reshaped the landscape of crime, giving rise to sophisticated forms of cybercrime. Key findings indicate that:

1. Emerging cybercrime trends: the study highlighted significant growth in cybercrimes like ransomware attacks, phishing, identity theft, and the exploitation of artificial intelligence (ai) to launch advanced cyberattacks. These threats continue to evolve, making traditional defence mechanisms increasingly ineffective.
2. Social engineering and human vulnerability: one major trend identified is the rise of social engineering techniques, where attackers exploit human psychology rather than technical vulnerabilities. Phishing and other forms of fraud often rely on deception rather than hacking infrastructure directly, underlining the importance of both technological solutions and public awareness in addressing cybercrime.
3. Global data protection laws: the study also found that regulatory frameworks such as the general data protection regulation (gdpr) in europe and the California consumer privacy act (ccpa) in the united states represent significant milestones in protecting individuals' privacy rights. However, despite these advancements, discrepancies between various national legal frameworks present challenges, especially in handling cross-border data flows and cybersecurity standards.
4. Gaps and challenges: despite advancements in data protection, the study revealed ongoing challenges in harmonizing international cyber laws and addressing emerging threats from new technologies like the internet of things (iot), ai, and cloud computing. Legislation often lags behind these rapidly evolving technologies, creating gaps that cybercriminals can exploit.

LegalOnus Law Journal (LLJ)

8.2. Recommendations for policy and legislation

Based on these findings, several recommendations can be made to strengthen the legal and regulatory landscape around cybercrime and data protection:

1. Global harmonization of cyber laws: one of the most pressing issues is the lack of unified global standards in combating cybercrime and protecting data. International bodies such as the United Nations and regional entities like the European Union should push for a more consistent and harmonized approach to cybercrime legislation, encouraging collaboration between countries for law enforcement and information sharing.
2. Regulation of emerging technologies: lawmakers should develop policies that address the unique risks posed by emerging technologies such as AI, machine learning, and IoT devices. Special attention must be given to the potential for AI to be used in automating cyberattacks and the vulnerabilities that arise from the proliferation of interconnected devices in everyday life. For example, specific regulations governing the security of IoT devices are needed to mitigate the risks posed by insecure smart devices.
3. Stronger data protection standards: data protection laws must evolve in response to modern cybersecurity threats. Governments should not only ensure stricter enforcement of existing laws like GDPR but also enhance the scope of these regulations to cover newer types of personal data (e.g., biometric and behavioural data) and extend liability for data breaches to third-party service providers.
4. Public awareness and education campaigns: in addition to technical and legal measures, public awareness campaigns should be a priority to reduce the success of social engineering attacks. Governments and businesses alike must invest in educating the public and employees about cyber threats, data protection rights, and how to recognize and respond to phishing and other malicious tactics.
5. Cross-border data protection agreements: given the global nature of cyberspace, policymakers should work toward cross-border agreements that provide consistent data

LegalOnus Law Journal (LLJ)

protection standards for personal data transferred between jurisdictions. Initiatives like the EU-u.s. Data privacy framework can be expanded to ensure global interoperability between different regulatory systems.

8.3. Final thoughts on the future of cybersecurity and data protection

Looking ahead, the battle between cybercriminals and cybersecurity experts will continue to intensify as both technology and threats evolve. The future of cybersecurity and data protection hinges on the ability of policymakers, businesses, and individuals to adapt to an ever-changing digital environment. Legislation must be forward-looking, anticipating emerging threats such as quantum computing, which has the potential to break current encryption standards, or the ethical concerns related to ai-driven decision-making.

Additionally, as more data is generated and stored online, the protection of personal and sensitive information will become even more critical. The challenge will be in striking the right balance between protecting individual privacy rights and fostering innovation in the digital economy. Data protection regulations must be flexible enough to adapt to new technologies while still providing robust safeguards for individuals.

Finally, international cooperation will play an essential role in the future of cybersecurity. Cybercrime knows no borders, and the global community must adopt a collective approach to develop consistent laws, share intelligence, and provide mutual legal assistance to fight cybercrime effectively.

As we move forward, the integration of ethical considerations into cybersecurity and data protection discussions will be crucial. Lawmakers and society must grapple with the implications of mass surveillance, data ownership, and the right to privacy in an increasingly connected world. Ultimately, the future of cybersecurity and data protection will depend on the ability of all stakeholders to navigate the complex trade-offs between security, privacy, and innovation in the digital age.

LegalOnus Law Journal (LLJ)

References

1. Brenner, s. W. (2019). Cybercrime and the law: challenges, issues, and outcomes. New York: northeastern university press..
2. Solove, d. J., & schwartz, p. M. (2020). Information privacy law (7th ed.). Aspen publishers.
3. Goodman, m. (2016). Future crimes: inside the digital underground and the battle for our connected world. New York: anchor books.
4. Clough, j. (2015). "a world of difference: the Budapest convention on cybercrime and the challenges of harmonisation." Monash university law review, 41(3), 682-713.
5. Goddard, m. (2017). "the EU general data protection regulation (gdpr): European regulation that has a global impact." international journal of market research, 59(6), 703-705.
6. Saxby, s. (2019). "data protection laws in the age of big data." computer law & security review, 35(1), 16-26.
7. Tropina, t. (2021). "the cybercrime ecosystem: global challenges and local responses." journal of information technology & politics, 18(3), 210-224.
8. European union. (2016). General data protection regulation (gdpr), regulation (EU) 2016/679 of the European parliament and of the council. California state legislature. (2018). California consumer privacy act (ccpa), assembly bill no. 375..
9. Council of europe. (2001). Convention on cybercrime (Budapest convention), etc no.185.
10. United nations office on drugs and crime (unodc). (2021). Comprehensive study on cybercrime.
11. Ibm security. (2023). Cost of a data breach report 2023.

LegalOnus Law Journal (LLJ)

12. World economic forum. (2022). Global cybersecurity outlook 2022.
13. McAfee & csis. (2020). The hidden costs of cybercrime.
14. Kaspersky labs. (2021). Cybercrime trends report 2021.
15. U.s. Department of justice. (2023). "computer crime and intellectual property section (ccips)."
retrieved from <https://www.justice.gov/criminal-ccips>
16. European data protection board (edpb). (2023). "guidelines on gdpr implementation."
retrieved from <https://edpb.europa.eu>
17. National institute of standards and technology (nist). (2022). Framework for improving critical infrastructure cybersecurity (version 1.1).
Retrieved from <https://www.nist.gov>
18. <https://www.academia.edu/resource/work/122392923>
19. <https://www.academia.edu/resource/work/116568734>
20. <https://www.academia.edu/resource/work/118946990>
21. <https://www.academia.edu/resource/work/122623515>

Legalonus

LegalOnus Law Journal (LLJ)

***CYBER FRAUDS AND THE LEGAL RESPONSE: A
COMPARATIVE ANALYSIS OF INDIA, THE US, AND THE
EU***
BY AGAM SHARMA

Legalonus

LegalOnus Law Journal (LLJ)

Abstract

This paper provides a comparative analysis of the legal frameworks addressing cyber fraud in India, the United States, and the European Union. The study evaluates each jurisdiction's response to cyber fraud, focusing on data protection and enforcement mechanisms. It also explores the challenges faced by these regions, including cross-border jurisdictional issues, the rapid evolution of fraud tactics, and the integration of emerging technologies in law enforcement. Drawing insights from the US and EU models, the paper offers recommendations for strengthening India's legal framework and enhancing global cooperation to combat cyber fraud effectively. Ultimately, it highlights the importance of adaptive, collaborative approaches in addressing the evolving landscape of cybercrime.

Keywords: cyber fraud, legal frameworks, data protection, cross-border jurisdiction, global cooperation.

I. Introduction:**a. Overview of cyber frauds.**

In today's digital world, cyber frauds have emerged as one of the most pervasive and dangerous forms of criminal activity. Cyber fraud encompasses a wide range of illicit practices that exploit technological platforms and the internet for financial or personal gain. These fraudulent activities often involve manipulating or stealing sensitive personal data, accessing secure financial systems, and conducting fraudulent transactions. As technology becomes more integrated into daily life, the scale of cyber fraud has escalated, affecting individuals, businesses, and governments globally. According to recent reports, the financial losses due to cybercrime are projected to reach billions of dollars annually, signaling a growing and urgent concern. The anonymity offered by the internet, combined with the rapid advancement of technology, makes cyber fraud particularly difficult to prevent and prosecute.

LegalOnus Law Journal (LLJ)

b. Importance of laws to address cyber frauds.

Given the increasingly sophisticated nature of cyber fraud, legal responses are essential for mitigating the risks and consequences of these crimes. Legal frameworks play a vital role in protecting citizens' rights, ensuring data security, and holding cybercriminals accountable. Laws addressing cyber fraud not only deter criminals but also provide victims with avenues for redress and recovery. A robust legal response is crucial for maintaining public trust in digital platforms, particularly as more individuals and businesses move online for banking, shopping, and communication.

In response to the growing threat, many countries have enacted specific laws to address cybercrime and data protection, creating a complex web of regulations. These legal frameworks aim to regulate the digital environment, secure personal data, and provide mechanisms for enforcement. However, the legal response to cyber fraud must constantly evolve to keep pace with technological developments and the increasingly global nature of cybercrime.

c. Research aims and scope.

This research paper seeks to conduct a comparative analysis of the legal frameworks addressing cyber frauds in India, the United States, and the European Union. By analysing these legal systems, the paper will explore the effectiveness of each jurisdiction's response to cyber fraud, focusing on data protection, enforcement mechanisms, and the balance between privacy and cybersecurity.

This study will also assess the challenges faced by these jurisdictions, such as cross-border jurisdictional issues, technological advancements by fraudsters, and the integration of emerging technologies in law enforcement. The ultimate aim is to identify best practices and make recommendations for enhancing India's legal framework to combat cyber fraud, drawing insights from the US and EU systems.

II. Types of cyber frauds, their prevalence and impact:

The different types of cyber fraud can be broadly categorized as follows:

LegalOnus Law Journal (LLJ)

1. Identity theft:

Identity theft is one of the most common forms of cyber fraud. It occurs when a cybercriminal unlawfully obtains and uses someone else's personal information, such as name, Aadhaar number, credit card details, or other identifying data, to commit fraud. Victims of identity theft may face financial losses, damage to their credit history, and difficulties in restoring their identity.

2. Phishing and spear phishing:

Phishing is a form of cyber fraud where attackers deceive individuals into divulging sensitive personal information by pretending to be a trustworthy entity, often via emails or fake websites. Spear phishing is a more targeted version, where the fraudster customizes the attack to a specific individual or organization, using information gleaned from social media or other sources to make the scam more convincing.

3. Online banking and credit card fraud:

Cybercriminals often target individuals or businesses through online banking fraud, which can involve unauthorized access to bank accounts, fraudulent transactions, or stealing login credentials through techniques like malware or phishing. Similarly, credit card fraud occurs when fraudsters obtain and misuse a person's credit card details for unauthorized transactions, often leading to financial losses for both consumers and financial institutions.

4. Ransomware attacks:

Ransomware is a type of malicious software (malware) that locks a user's computer or encrypts their files, holding them hostage until a ransom is paid. Cybercriminals often target businesses, government agencies, or individuals with critical data. If the ransom is not paid, the data may be deleted or permanently held hostage, causing significant disruption to operations and data loss.

5. Business email compromise (bec):

LegalOnus Law Journal (LLJ)

Bec scams involve attackers posing as a company executive, vendor, or trusted partner to trick employees into transferring money or sensitive information. These types of scams are particularly dangerous for businesses because they often bypass traditional security systems by exploiting the trust and authority associated with organizational leaders.

6. Social media and online auction fraud:

With the growing use of social media platforms and online marketplaces, cybercriminals have increasingly targeted users by creating fake profiles or fraudulent online ads. In online auction fraud, fraudsters deceive individuals into paying for goods or services that do not exist, while social media fraud often involves scams such as fake giveaways, impersonation, and fraudulent investment opportunities.

7. Cryptocurrency fraud:

As the popularity of cryptocurrencies has surged, so has the incidence of crypto-related frauds. These scams include Ponzi schemes, fake initial coin offerings (icos), and fake crypto exchanges that promise high returns but disappear with investors' funds. Fraudulent cryptocurrency transactions are difficult to trace due to the pseudo-anonymous nature of many blockchain platforms.

Prevalence and impact

The prevalence of cyber frauds has grown exponentially in recent years, as more individuals and organizations shift towards online platforms for personal and business activities. As of 2023, global reports indicate that cybercrime, including fraud, has become one of the largest threats to economic and social stability, with losses running into billions of dollars annually. The ease of access to digital platforms, combined with the increasing sophistication of cybercriminals, has made it difficult to track and prevent these crimes.

According to the cybersecurity and infrastructure security agency (cisa), cybercrime is responsible for financial losses of over \$10 trillion globally, a number expected to grow substantially in the

LegalOnus Law Journal (LLJ)

coming years. The FBI's internet crime complaint center (IC3) reported over 800,000 complaints related to cyber fraud in the United States alone in 2022, with reported financial losses exceeding \$7 billion. In India, the National Crime Records Bureau (NCRB) has documented a steady increase in the number of cybercrimes, with cyber frauds forming a significant portion of these statistics. The rise in online transactions, particularly during and after the COVID-19 pandemic, has further exacerbated the situation.

III. Legal framework in India for addressing cyber frauds:

India's legal framework for addressing cyber frauds is primarily shaped by the Information Technology Act, 2008 (IT Act) and the upcoming Digital Personal Data Protection Act, 2023 (DPDPA). These laws aim to protect citizens and organizations from digital fraud, safeguard personal data, and strengthen enforcement mechanisms.

The digital personal data protection act, 2023 (DPDPA)

Though yet to be implemented, the Digital Personal Data Protection Act, 2023 (DPDPA) is India's most recent and comprehensive legislation aimed at regulating the processing of personal data, addressing privacy concerns, and protecting individuals from the misuse of their data. The DPDPA replaces the Personal Data Protection Bill, 2019, which had been stalled in Parliament. The passage of the DPDPA signifies a major shift in India's approach to data privacy and security, responding to growing concerns about data breaches and cyber fraud.

Key provisions of the DPDPA related to cyber frauds include:

1. Data protection and fraud prevention:

The DPDPA establishes a robust framework for data protection, requiring organizations to obtain explicit consent from individuals before processing their personal data. This provision directly

LegalOnus Law Journal (LLJ)

impacts cyber fraud, as it strengthens controls over the collection and storage of sensitive personal information. By restricting unauthorized access and use of personal data, the law aims to mitigate identity theft, phishing attacks, and other forms of cyber fraud involving data misuse.

2. Breach notification:

One of the central features of the dpdpa is the requirement for data fiduciaries (those who control or process personal data) to notify both the data protection board of india (dpbi) and affected individuals in the event of a data breach. Prompt notification allows individuals to take action to safeguard their financial and personal data, reducing the impact of potential fraud.

3. Rights of individuals:

The dpdpa grants individuals specific rights, such as the right to access, right to correction, right to erasure, and right to data portability. These rights empower individuals to control their personal data, which is crucial in preventing fraud. For instance, if a person's data is compromised or misused, they have the right to request the deletion or rectification of that data, thereby minimizing the chances of further fraudulent activity.

4. Accountability and penalties:

The dpdpa imposes stringent penalties on organizations that fail to comply with its provisions, including hefty fines for non-compliance with data protection requirements. These provisions incentivize companies to invest in stronger cybersecurity measures, reducing vulnerabilities that could lead to fraud.

Although the dpdpa is a significant step forward in addressing data protection, its effectiveness will depend on the speed of enforcement, awareness campaigns, and inter-agency coordination to deal with emerging fraud techniques.

LegalOnus Law Journal (LLJ)

The information technology act, 2000 (it act)

As on date, the information technology act, 2000 (it act) is the primary law in india for addressing cybercrimes, including cyber frauds. It was one of the first comprehensive laws to address the legal aspects of cybercrime in india. Key provisions related to cyber frauds under the it act include:

1. Section 66c (identity theft):

This section criminalizes the use of someone else's identity or digital signature to commit fraud. It applies to various frauds where fraudsters impersonate individuals to gain access to financial accounts or cause harm to personal reputations. The penalty for identity theft under section 66c includes imprisonment and fines.

2. Section 66d (cheating by impersonation):

Section 66d deals with cheating and fraud through the use of communication devices, including mobile phones, emails, or websites. It criminalizes the act of deceiving someone into providing money or information through false representation. This section is particularly relevant in addressing frauds like online phishing, romance scams, and other internet-based scams where victims are manipulated into providing financial information or transferring money.

3. Section 43b (accessing protected systems):

This provision addresses unauthorized access to computer systems or data and is applicable to cyber frauds where criminals gain unauthorized access to sensitive data, like banking information or private documents. It imposes penalties for such actions, including fines.

4. Section 72a (punishment for disclosure of information in breach of law):

This section criminalizes the disclosure of personal information in breach of confidentiality agreements. It is relevant in cases where cyber fraud involves the misuse or theft of personal data, such as the unauthorized sharing of credit card information or banking details.

LegalOnus Law Journal (LLJ)

While the it act offers a comprehensive framework for prosecuting cyber frauds, challenges remain in its implementation. The law does not fully address newer forms of cybercrime like ransomware and cryptocurrency fraud, and its provisions on data protection were found to be inadequate, leading to the introduction of the dpdpa.

IV. Legal framework in the us for addressing cyber frauds:

The united states has a multi-layered legal framework for addressing cyber frauds, drawing from federal laws, regulatory agencies, and state-specific legislation. Key components include the computer fraud and abuse act (cfaa), the role of the federal trade commission (ftc) in consumer protection, and state-specific laws like the California consumer privacy act (ccpa)

The computer fraud and abuse act (cfaa) (1986)

The cfaa is a foundational federal law addressing computer-related fraud and abuse. Initially enacted to combat hacking, it has evolved to cover a wide range of cybercrimes, including fraud using computer systems. The key provisions are:

1. Unauthorized access to computer systems: the cfaa criminalizes unauthorized access to protected computer systems, including using deception or fraud to gain access (e.g., hacking into financial systems).
2. Fraud and misuse of information: the law specifically targets instances where individuals access computers to commit fraud or steal sensitive information. This includes the use of phishing schemes to obtain login credentials and other financial frauds.
3. Damaging systems or data: it also criminalizes the intentional damaging of data or systems, which may be linked to fraudulent activities such as deleting financial records or spreading malware.

LegalOnus Law Journal (LLJ)

While the cfaa was originally designed to target hacking and unauthorized access, its broad language has also been used to address cyber fraud activities, such as exploiting weaknesses in online banking systems or stealing sensitive financial data.

Federal trade commission (ftc) and consumer protection laws

The ftc plays a crucial role in regulating cyber fraud, particularly in terms of consumer protection. The agency enforces laws and regulations aimed at safeguarding consumers from financial fraud, identity theft, and other online scams.

1. Role of the ftc in cyber fraud: the ftc investigates and takes action against fraudulent practices that target consumers, including deceptive marketing, identity theft, and phishing scams. It educates consumers about how to avoid cyber fraud and provides resources for reporting fraud, as well as offering tools to assist victims in recovery.
2. Identity theft and assumption deterrence act (1998): this act, enforced by the ftc, specifically targets identity theft, a major form of cyber fraud. It criminalizes the act of knowingly using another person's identity without authorization to commit fraud. It requires federal agencies and businesses to take steps to prevent identity theft, such as the implementation of data security measures, and allows individuals to place fraud alerts on their credit reports to prevent further misuse of their identities.

State-specific laws (e.g., California consumer privacy act - ccpa)

While federal laws set broad standards, states like California have implemented additional measures to protect residents from cyber fraud and ensure privacy in the digital age.

- California consumer privacy act (ccpa)

LegalOnus Law Journal (LLJ)

Enacted in 2018, the ccpa provides California residents with enhanced control over their personal data. Although primarily a privacy law, its provisions help address cyber fraud by imposing strict requirements on businesses that collect, use, and share personal information. Key features of this act are:

1. Consumers have the right to know what personal information is being collected and to request that their data be deleted.
 2. The law mandates businesses to implement reasonable security measures to protect consumer data from unauthorized access and fraud.
 3. It also allows consumers to opt-out of the sale of their personal information, reducing the risk of data breaches and subsequent fraud.
- Other states have also enacted similar laws, including the new York shield act (requiring businesses to protect private information), and Virginia's consumer data protection act (cdpa), further strengthening protections against cyber fraud at the state level.

V. Legal framework in the EU for addressing cyber frauds:

The European union (EU) has developed a robust legal framework for addressing cyber fraud, combining privacy protections, cybersecurity measures, and criminal sanctions. Key legal instruments that help mitigate and prevent cyber fraud include the general data protection regulation (gdpr), the EU cybersecurity act (2019), and the EU directive on attacks against information systems (2013). Together, these regulations empower individuals, businesses, and law enforcement authorities to address the growing threat of cyber fraud and enhance the EU's overall cybersecurity resilience.

General data protection regulation (gdpr)

LegalOnus Law Journal (LLJ)

The gdpr, which came into force in May 2018, is one of the most comprehensive data protection laws in the world. While its primary purpose is to protect the personal data and privacy of EU citizens, it also plays a critical role in preventing cyber fraud by mandating robust safeguards for data security and establishing clear rights for individuals. The key provisions of the gdpr are:

1. Notification of a personal data breach to the supervisory authority (article 33): this article mandates that organizations report personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach. A data breach is any incident leading to unauthorized access to, disclosure of, or loss of personal data. For cyber fraud prevention, this means that organizations must promptly alert regulators if a breach occurs, ensuring that malicious actors exploiting vulnerabilities (e.g., hackers or fraudsters) are identified and investigated quickly.
2. Communication of a personal data breach to the data subject (article 34): when a data breach is likely to result in a high risk to the rights and freedoms of individuals (e.g., exposure of sensitive financial or identity data), the organization is also required to notify affected individuals without undue delay. This empowers consumers to take precautionary measures, such as freezing accounts or changing passwords, to mitigate the risk of fraud.
3. Empowering individuals to prevent the misuse of personal data: the gdpr also provides several rights to individuals that directly help prevent the misuse of their personal data, which is often a primary tool in cyber fraud. These rights include:
4. Right to access (article 15): individuals have the right to obtain confirmation from organizations on whether their personal data is being processed. This allows individuals to ensure that their data is not being used fraudulently.

LegalOnus Law Journal (LLJ)

5. Right to rectification (article 16): if personal data is inaccurate, individuals can request that it be corrected, preventing fraudsters from exploiting incorrect information.
6. Right to erasure (article 17): also known as the "right to be forgotten," this right allows individuals to request the deletion of personal data when it is no longer necessary for the purposes for which it was collected, or when it has been unlawfully processed. This provision is particularly useful in preventing fraud that relies on outdated or unnecessary data.

Eu cybersecurity act (2019)

The EU cybersecurity act (regulation (EU) 2019/881) was adopted to strengthen the EU's cybersecurity capabilities and provide a unified approach to tackling cyber threats, including cyber fraud. It lays the foundation for a European cybersecurity certification framework, improving the security of products, services, and processes across the EU. This act plays a central role in enhancing the EU's ability to prevent and respond to cyber fraud by:

1. Creating the European cybersecurity agency (enisa): the act strengthens enisa by giving it a more central role in coordinating cybersecurity efforts across EU member states. This enables the agency to better support national governments in dealing with cyber fraud, share best practices, and provide cybersecurity expertise.
2. Cybersecurity certification: the act establishes an EU-wide cybersecurity certification framework for products and services, which helps ensure that companies meet high security standards, reducing vulnerabilities that fraudsters could exploit. For example, cybersecurity certification of financial platforms or digital payment systems ensures that they are secure against fraud and other cyberattacks.
3. Eu cybersecurity risk management: the act also introduces requirements for critical sectors (e.g., finance, energy, healthcare) to adopt comprehensive risk management practices and report serious incidents. These measures ensure that organizations are

LegalOnus Law Journal (LLJ)

better prepared to prevent cyber fraud by strengthening their defences against potential attacks.

EU directive on attacks against information systems (2013)

The EU directive on attacks against information systems (directive 2013/40/EU) criminalizes a range of cybercrimes, including those related to cyber fraud. It is one of the most important pieces of legislation in the EU aimed specifically at tackling cybercrime and fraud in the digital age. The directive sets out common minimum standards for the criminalization of attacks against information systems, which is particularly relevant in the context of cyber fraud. It targets activities such as:

- Hacking: unauthorized access to computer systems to steal or alter data for fraudulent purposes.
- Phishing: deceptive practices where fraudsters impersonate legitimate organizations to trick individuals into revealing sensitive personal data (e.g., banking credentials).
- Denial of service (dos) attacks: disabling websites or online services to create opportunities for fraud, extortion, or other malicious activities.
- Malware and ransomware: distributing malicious software to steal information or hold systems hostage for financial gain.

VI. Comparative analysis of legal frameworks in india, the us, and the EU:

This comparative analysis will evaluate the legal frameworks in these three jurisdictions in terms of scope, enforcement mechanisms, technological integration, jurisdictional issues, international cooperation, and the balance between privacy and security.

1. Scope and coverage:

LegalOnus Law Journal (LLJ)

- **India:** India's legal framework for cyber fraud is evolving, with cybercrime and data protection laws being progressively updated. Initially governed by the information technology act, 2000 (it act), which criminalizes cyber fraud, the framework was updated with the digital personal data protection act, 2023 (dpdpa). The it act addresses offenses like hacking, identity theft, and data breaches, but it lacks provisions for newer forms of cyber fraud, such as fraud involving cryptocurrencies or ai-driven scams. The dpdpa, enacted in 2023, aims to modernize India's data protection regime by introducing more stringent measures for handling personal data. It enhances the regulatory framework for data breaches, including stronger obligations for data controllers to secure data and notify data subjects in case of breaches. However, India's cybercrime laws still face challenges in keeping up with the increasingly sophisticated nature of cyber fraud.
- **United states:** the us boasts a comprehensive framework for cyber fraud, particularly through laws like the computer fraud and abuse act (cfaa), the identity theft and assumption deterrence act (1998), and various sector-specific regulations (e.g., hipaa for healthcare fraud). These laws cover a wide array of cyber fraud activities, from hacking and phishing to identity theft and fraud through financial systems. Despite its robust regulatory landscape, the us suffers from a fragmented approach, as federal, state, and sector-specific laws sometimes lead to overlaps or gaps in enforcement.
- **European union:** the EU has developed a unified, multi-faceted legal framework, with core regulations such as the general data protection regulation (gdpr), the EU cybersecurity act (2019), and the EU directive on attacks against information systems (2013). The gdpr addresses data protection and security breaches, while the cybersecurity act strengthens the EU's cybersecurity framework by certifying critical infrastructure and digital products. This integrated approach makes the EU's

LegalOnus Law Journal (LLJ)

framework one of the most comprehensive, particularly in balancing privacy protections with fraud prevention.

2. Enforcement mechanisms:

- India: enforcement in india is still evolving. While the cybercrime cells exist at both the state and national levels, they face challenges in terms of capacity, resources, and training. The judicial system is slow in addressing cybercrime cases, and public awareness about how to report cyber fraud remains limited.
- United states: the us has specialized agencies like the federal bureau of investigation (fbi) and secret service, which are highly effective in investigating and prosecuting cyber fraud. Additionally, the federal trade commission (ftc) plays a significant role in protecting consumers from identity theft and financial fraud. However, coordination between federal, state, and local authorities can sometimes be a bottleneck in addressing multi-state or multi-jurisdictional cyber fraud cases.
- European union: the EU benefits from a strong enforcement framework, primarily through Europol and its European cybercrime centre (ec3), which coordinate cross-border investigations. National law enforcement agencies are well-equipped to handle cyber fraud, but enforcement can sometimes be delayed due to differing legal standards across member states. The gdpr enforcement is also handled by national data protection authorities (dpas), but enforcement can vary depending on the country's commitment to compliance.

3. Technological integration in legal responses:

- India: India's law enforcement agencies are still catching up in terms of integrating digital forensics into cyber fraud investigations. While there are some cyber labs in

LegalOnus Law Journal (LLJ)

the country, the use of ai and machine learning (ml) is not widespread. The cybercrime cells use traditional forensic methods, which are often slow and insufficient for handling modern, complex cyber frauds.

- United states: the us is a leader in integrating ai, machine learning, and digital forensics into cyber fraud detection and prevention. The fbi uses advanced ai tools to track down cybercriminals, and financial institutions employ ai-driven systems to detect fraudulent transactions in real time. The private sector also plays a key role in innovating fraud prevention technologies.
- European union: the EU has also made significant strides in incorporating ai and ml into fraud detection, especially through the cybersecurity act and efforts coordinated by Europol. The EU emphasizes ethical considerations in the use of ai for fraud prevention, particularly in relation to gdpr's privacy concerns.

4. Jurisdictional issues and international cooperation:

- India: india is a signatory to the Budapest convention on cybercrime, which facilitates international cooperation in cybercrime cases. However, India's capacity to effectively engage in cross-border cyber fraud prosecutions is limited by gaps in its enforcement mechanisms and slow judicial processes. The dpdpa addresses cross-border data flows but is still un-tested in addressing jurisdictional issues in cybercrime.
- United states: the us has a well-established framework for cross-border cooperation in cyber fraud cases, facilitated through the Budapest convention, Interpol, and other international agreements. However, differences in legal frameworks and enforcement practices between countries can create barriers in pursuing international cyber fraud cases.

LegalOnus Law Journal (LLJ)

- European union: the EU's framework for cross-border cybercrime is robust, with Europol and national authorities collaborating effectively through mutual legal assistance treaties (mlats) and other tools. The EU's single market and cohesive legal structure enhance its ability to prosecute cross-border cyber fraud.

5. Privacy vs. Security:

- India: India's privacy laws have been evolving, with the digital personal data protection act, 2023 (dpdpa) setting new standards for personal data protection. While the dpdpa focuses on strengthening data security, it also permits certain data processing for law enforcement purposes, which may raise concerns regarding the privacy-security balance.
- United states: the us prioritizes security over privacy in its approach to cyber fraud. Laws like the cfaa allow extensive data surveillance, often for security purposes, but this can lead to concerns about civil liberties and the potential for overreach in the name of fraud prevention.
- European union: the gdpr is at the forefront of privacy protection, but it also allows for the processing of personal data for purposes of fraud detection and prevention, provided that it complies with strict safeguards. The EU emphasizes the importance of maintaining individual privacy while also ensuring that data can be used to prevent cyber fraud.

Legalonus

VII. Conclusion:

a. Summary of key findings:

The comparative analysis of the legal frameworks in india, the united states, and the European union highlights both the strengths and weaknesses of each jurisdiction's response to cyber fraud. In india, the introduction of the digital personal data protection act, 2023 (dpdpa) represents a

LegalOnus Law Journal (LLJ)

significant step towards improving data protection and mitigating cyber fraud. However, it is yet to be tested and its enforcement will remain a challenge due to gaps in infrastructure, legal clarity, and technological capacity. The us legal landscape is more robust in addressing cybercrime, with a strong emphasis on data breach notifications and consumer rights. However, the fragmented nature of us laws and the challenges posed by varying state laws can create inconsistencies in enforcement. The EU's legal framework, provides a comprehensive and unified approach to data protection and cybersecurity, with a strong focus on cross-border cooperation. However, the complexity of EU regulations may sometimes result in bureaucratic hurdles and enforcement delays.

Across all jurisdictions, a common challenge is the constant evolution of fraud tactics, which outpaces the legislative response. While india and the us are still catching up in terms of technological enforcement mechanisms, the EU benefits from a more coordinated regulatory approach but struggles with maintaining flexibility to adapt to rapidly evolving threats.

b. Recommendations for india:

Based on the strengths of the legal frameworks in the us and EU, several improvements can be made to India's legal framework for combating cyber fraud.

- **Cross-border cooperation:** india should enhance its international cooperation mechanisms for tackling cyber fraud. This can be achieved through better integration with global frameworks such as the Budapest convention on cybercrime, ensuring easier information sharing, and enhancing cooperation with foreign law enforcement agencies. The EU cybersecurity act and the cfaa provide useful models in this regard, with their emphasis on multilateral collaboration in the fight against cybercrime.
- **Improved data breach notification systems:** India's dpdpa would benefit from a more explicit and stringent data breach notification system, similar to the ccpa. This would ensure that organizations are legally compelled to

LegalOnus Law Journal (LLJ)

notify affected individuals in a timely manner, increasing transparency and accountability. Clear timelines and consequences for non-compliance would further strengthen the framework.

- Digital forensics and enforcement capacity: india should invest in digital forensics capabilities and specialized training for law enforcement. Drawing inspiration from the use's approach, india can improve its technical capacity to handle complex cyber fraud investigations, particularly by establishing dedicated cybercrime units and increasing the use of ai and blockchain in tracing and preventing fraudulent activities.

c. The future of cyber fraud prevention:

The future of cyber fraud prevention will increasingly depend on the integration of emerging technologies, global cooperation, and evolving legal frameworks. Technologies such as artificial intelligence (ai) and blockchain hold tremendous potential to transform the fight against cyber fraud. Ai can assist in detecting anomalies and predicting fraud patterns, while blockchain's decentralized nature could be leveraged to create tamper-proof records for transactions, enhancing transparency and trust.

However, these technologies also present new challenges, including the potential for fraudsters to exploit ai in their schemes or to find ways to circumvent blockchain's security features. Additionally, the rise of quantum computing could eventually undermine the encryption protocols currently used in fraud prevention, demanding a proactive approach from lawmakers and regulators to prepare for such disruptions.

On the global stage, cyber fraud continues to be a cross-border issue that requires strong international coordination. The EU's focus on cooperation through the gdpr and its collaborative approach with international bodies is an example that other countries, including india, can adopt to address the borderless nature of cybercrime. Cross-border jurisdictional issues must be tackled

LegalOnus Law Journal (LLJ)

through the establishment of clearer international legal standards, faster extradition processes, and mutual recognition of cybercrime-related evidence.

In conclusion, while the legal frameworks of india, the us, and the EU each offer valuable insights, the fight against cyber fraud requires an evolving, flexible, and technologically-savvy approach. By learning from the best practices of these jurisdictions and preparing for the challenges of emerging technologies, india can build a more robust legal infrastructure to combat cyber fraud effectively and ensure the protection of its citizens in the digital age.

References:

1. Solove, daniel j., & schwartz, paul m. (2021). Information privacy law. 7th edition. Aspen publishers.
2. Kuner, christopher. (2020). The general data protection regulation: a commentary. Oxford university press.
3. Lindsay, jonathan r., & reiger, david a. (2022). "the evolution of cybercrime and its legal responses: a comparative perspective." journal of cybersecurity law, 10(3), 45-78.
4. Vaghela, b. P., & shah, j. (2023). "cybercrime and legal framework in india: a new paradigm." Indian journal of cyber law, 6(1), 32-50.
5. Ministry of electronics and information technology (meity), government of india. (2023). Digital personal data protection act, 2023.
6. European commission. (2019). Eu cybersecurity act (regulation (EU) 2019/881). Official journal of the European union.
7. United states congress. (1986). Computer fraud and abuse act (cfaa). Public law no: 99-474.

LegalOnus Law Journal (LLJ)

8. California state legislature. (2020). California consumer privacy act (ccpa). California civil code, section 1798.100 et seq.
9. Indian computer emergency response team (cert-in). (2023). Annual cybersecurity threat report.
10. World economic forum (wef). (2022). Global risks report: the rise of cybercrime and fraud.



Legalonus

Maiden Issue

S. No.:	Particulars	Details
1.	Place of publication	Lucknow, Uttar Pradesh
2.	Language	English only
3.	Under the guidance	Mr. Anandh Kumar V
4.	Owner, & Publisher	LEGALONUS LAW JOURNAL, Ayush Chandra, Lucknow, UP, India

Guidelines for Contributors

- Original accounts of research in the form of articles, short articles, reports, notes, comments, review articles, book reviews and case comments shall be most appreciated. • Mode of citation: Footnotes, References
- Font; Times New Roman
- Font size: 12 points for text and 10 points for footnotes.
- Spacing: 1.5
- Mode of Submission: Email
- Email: journal@legalonus.com