*A Quarterly insight to Cyber Law!*

*Cyber Niyam means rules of the Cyberspace. This quarterly newsletter aims to create awareness about the rules and regulations of cyberspace, cyber security and data protection. This is also an effort to create awareness about digital safety, trending cybercrimes and effective reporting mechanisms.*



V.P SHINTRE & ASSOCIATES
Legacy since 1935.

# CYBER NIYAM


*By V.P Shintre & Associates* *www.vaishalibhagwat.com*



**Issue 2 of 2025 – April, 2025**


## In this Issue



## TRENDING CYBER FRAUDS

### *Online Share Market Scams – How it works and Preventive Measures*

Cyber frauds have become rampant and very dynamic recently. Due to the variety in conducting these frauds people find it difficult to predict or be cautious all the time. One such type is the Share trading scams. These often result in significant financial losses for investors. Deceptive practice such as manipulating stock prices is used to defraud individuals of their money. In order to identify a share trading scam and get out of the situation, a user must understand the various ways through which fraudsters carry out them.

**Pump and Dump Scheme**

Fraudsters artificially inflate the price of a stock (the "pump") by spreading misleading information or hype, often disseminated via social media or other online forums. Once the stock price is up due to the misinformation spread, the scammers sell their shares at a profit (the "dump"), other investors lose a lot of money, leaving them with worthless stocks when the price inevitably crashes.

**Boiler Room Frauds**

Brokers use high-pressure sales techniques like cold calling people pressuring them into buying low quality or non-existent stocks. They pressurize investors in making rushed decisions to buy low quality or non-existent shares. Boiler room frauds start with unsolicited phone calls from scammers who sound like professional "stockbrokers" persuading victims to agree to buy shares.




.....Continued on page 2

**Fake Investment Platforms**
Fake investment platforms mimicking legitimate trading sites often lure victims into investing through these platforms, only to find their funds are inaccessible at the time of withdrawal. Scammers create and use fraudulent apps to siphon off millions from investors by displaying fictitious profits.

**How it all starts**

1. Victims receive unsolicited calls from individuals claiming to be investment brokers offering attractive opportunities.
2. Scammers establish credibility by sharing fake success stories, projecting fake profits to the investments made and fake testimonials from supposed satisfied clients.
3. Victims are then encouraged or pressured to invest quickly to capitalize on purportedly high returns, often being added to WhatsApp groups for ongoing communication.
4. Once funds are deposited by the victim into fake accounts, they project fabricated growth figures on their investments.
5. When an attempt to withdraw funds is made, they are met with various excuses requiring them to pay additional fees or taxes, further entrenching them in the scam

**SECURITIES AND EXCHANGE BOARD OF INDIA (STOCK BROKERS) REGULATIONS GUIDELINES for people to caution**

In a caution to public notice issued by SEBI on 5th December, 2024 PR. No. 32/2024; SEBI has urged to exercise caution in undertaking transactions on unregistered platforms. It has advised investors to not engage with or undertake investment or trading activities through un-registered intermediaries/web applications/ platforms/apps.

**How to prevent from falling for these scams?**

1. Ensure that the investment platform and the broker is duly registered with SEBI
2. Independently verify the investment options rather than blindly trusting unsolicited advice
3. When offered unrealistic high returns be sceptical about such offers as investments with little to no risks are often indicative of fraudulent intentions.
4. Always check for the receipt of the investments made and are from the authentic sources/organization.

**Effects and Repercussions**
The impact of these scams extends beyond financial losses. Victims often suffer significant financial setbacks, which can lead to long-term economic hardship. Such scams contribute to a broader erosion of trust in financial markets and investment opportunities, making it harder for legitimate businesses to attract investors. Victims are traumatized for life because of the large sum of money lost, which is usually either their savings or a loan taken out.

**Conclusion**
These scams are a significant threat to investors as these could potentially lead to huge financial losses even taking a toll on one's wellbeing. By familiarizing yourself with the fraudulent schemes and the preventive measures you can better recognize and avoid such potential harms.



## GOOD TO KNOW!

### National Cyber Crime Helpline

Helpline number – 1930

Website - https://cybercrime.gov.in/

### National Cyber Crime Reporting Portal

Website - https://cybercrime.gov.in/

This portal allows you to file a complaint online and track its status

If you've registered a complaint using the "Report & Track" option and the response isn't satisfactory, contact the respective State/UT Nodal Officer or Grievance Officer.

# LEGAL LANDSCAPE

## *Balancing Privacy and Free Speech – Right to be Forgotten and Judicial Decisions*

The need for right to be forgotten arises when historically accurate information put on the internet starts affecting one's well-being, outweighing the interest of the world maintaining an online archive. Right to be forgotten is a claim by an individual to erase certain truthful accurate data from the internet preventing from third persons or persona non grata from accessing information which is detrimental to the image of a person. Synonymously used with 'Right to be erased' is a person's right to request removal of certain information about them floating around the internet.

**Origin**

le droit a l'oubli i.e. Right to Oblivion in French Jurisprudence originally refers to the idea that individuals should have the right to move on from their past, particularly in cases where past actions or events no longer reflect their current character or circumstances. The modern meaning given to this concept is that this right gives people the legal means to obtain the right to forget their personal or information related which has no relevance in the present from the internet

In 1998, Mario Costeja González, a Spanish national, faced significant financial troubles and urgently needed money. To address this, he listed a property for auction in a newspaper, and the advertisement inadvertently found its way onto the internet. Unfortunately, the digital world did not let go of this information. Years later, even after González had resolved his financial problems, details about the auction remained easily accessible through Google searches. This led people who looked him up to mistakenly believe he was still in financial ruin. The persistent association with bankruptcy caused considerable harm to his reputation, compelling him to pursue legal action. This landmark case eventually led to the establishment of the "right to be forgotten" principle

**General Data Protection Regulation**

GDPR recognizes Right to be forgotten as 'Right to erasure 'that is an individual's right to get certain data erased from the internet.

**Article 17 -** under following conditions erasure can be requested:

1. Data collected is no longer necessary to be processed,
2. Where the data subject withdraws his/her consent, the data subject objects processing of such data
3. Where the personal data has been unlawfully processed
4. The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject or when the data subject was a minor when such data was collected.

**Article 19** requires data controllers to notify all recipients about any rectification, erasure, or restriction of processing of personal data that has been carried out. However, no right is absolute, The Right to Erasure is not absolute and is subject to certain limitations. Data cannot be erased in the following cases:

a. Exercising freedom of speech and expression
b. For compliance with legal obligations
c. For reasons of public interest and public health
d. For the defence of legal claims

**In India**

**DPDP Act, 2023**

Section 8 (7)(a) of the DPDP Act, 2023 states that A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force, —

(a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and
(b) cause its Data Processor to erase any personal data that was made available
by the Data Fiduciary for processing to such Data Processor.
(8) The purpose referred to in clause (a) of sub-section (7) shall be deemed to no
longer be served, if the Data Principal does not—
(a) approach the Data Fiduciary for the performance of the specified purpose;
And
(b) exercise any of her rights in relation to such processing, for such time period as may be prescribed, and different time periods may be prescribed for different classes of Data Fiduciaries and for different purposes.
Section 12 Right to correction and erasure of personal data.
(1) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (a) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(2) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal, —
(a) correct the inaccurate or misleading personal data;
(b) complete the incomplete personal data; and
(c) update the personal data.

(3) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force

DPDP Act creates a framework where individuals can have their data erased either by withdrawal of consent, when the purpose expires or upon direct request. Here, the Data Fiduciary must ensure their processors erase data too, which is similar to GDPR's processor obligations. Similar to article 17(1)(a) and (b) of the GDPR, DPDP Act, 2023 aligns with the Right to be Forgotten principle of GDPR requiring erasure when consent is withdrawn and when data is no longer necessary for original purpose.

However, the DPDP Act avoids the term "Right to Be Forgotten," focusing instead on procedural erasure obligations. The Act lacks clarifications on the mechanisms to implement consent withdrawal, expiry and direct request.

**The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**

Rule 3 (2) (d) states that the upon receipt of complaint for removal of information to the Grievance Officer shall act expeditiously within 72 hours of such reporting.

As per Rule 3(1) The intermediary shall remove information either voluntarily or on receipt of a complaint if such information:

i. Belongs to another person and to which the user does not have any right.
ii. Content that is obscene, pornographic, invasive of privacy, insulting, harassing, racially or ethnically offensive, promotes money laundering or gambling, causes harm through online gaming, or incites violence between religious or caste groups.
iii. Is harmful to child
iv. Infringes any patent, trademark, copyright or other proprietary rights
v. Includes communication of misinformation
vi. Impersonates another person
vii. Content that threatens India's unity, security, sovereignty, foreign relations, public order, or obstructs law enforcement
viii. Contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource
ix. Promotion or advertisement of unverified or non-permissible online games.
x. Violates any law for the time being in force;

**Judicial Precedents**
Before 2021 due to lack of appropriate provisions support of judicial precedents had to be taken to understand whether one can avail for Right to be Forgotten.

In the case of ***State of Punjab v. Gurmeet Singh and Ors. (1996)*** the court stated that "*The Courts should, as far as possible, avoid disclosing the name of the prosecutrix in their orders to save further embarrassment to the victim of sex crime. The anonymity of the victim of the crime must be maintained as far as possible throughout*."

In **2017, Hon'ble Supreme Court of India in *K.S. Puttaswamy and Anr vs. Union of India and Ors***, ("**Puttaswamy Judgment**"), asserting that the *right to privacy is a fundamental right* enshrined under Article 21 of the Constitution and includes the right to be forgotten.

In the case of **Sri Vasunathan v. The Registrar General & Ors (2017)** the Hon'ble Karnataka High Court stated that "*This would be in line with the trend in western countries of the 'right to be forgotten' in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned*"

In **Jorawar Singh Mundy V. Union of India and Ors. (2021)** The Petitioner is an American citizen by birth having an Indian origin. When he travelled in 2009 to India, a case under the Narcotics Drugs and Psychotropic Substances Act, 1985, was lodged against him. In April 2011, the trial court acquitted him of all the charges. The Petitioner stated that after returning to the US and graduating from law school he was still unable to get a job as recruiters would find the case on the internet.

The court stated that:
*"Owing to the irreparable prejudice which may be caused to the Petitioner, his social life and his career prospects, in spite of the Petitioner having ultimately been acquitted in the said case via the said judgment, prima facie this Court is of the opinion that the Petitioner is entitled to some interim protection, while the legal issues are pending adjudication by this Court."*

In ***Karthick Theodore vs. The Registrar General, Madras HC, IKanoon Software Development Private Limited, and Ors,***

A writ of Mandamus was filed by Karthick Theodore seeking redaction of this name from the publicly accessible judgement where he was acquitted. The Applicant argued that the online availability of the judgement is causing significant harm to his reputation and thereby requested the court to mask his name, claiming protection under right to privacy, particularly the right to be forgotten. The Madras High Court allowed the writ appeal and ordered the Respondents to take down the judgement wherein his personal details were available and to redact the name and details of the Applicant. However, the details of the Applicant shall not be removed from the court records.

In the appeal the CJI raised concern questioning how a publicly available judgement could be ordered to be taken down as a judgement once delivered becomes part of the public record. In the said case the Supreme Court instructed Ikanoon Software Development Pvt Ltd to remove the copy of the judgment from their website. Additionally, it directed the Madras High Court registry to redact the individual's name and any identifying details from the judgment, ensuring that only the redacted version is published and uploaded.

From the above case laws, it can be understood that the court respects ones right to be forgotten and understands the harsh consequences on the individual when certain data is made available on the internet.

**Challenges of Right to be Forgotten**

One of the setbacks of Right to be Forgotten is that it can potentially degrade the quality of search results. If a news article about a person is delisted from the internet users may loose on important contextual information. This creates a tussle between an individual's right to information and one's right to privacy. When data is removed or delisted due to Right to be Forgotten, it may affect the accuracy and reliability of the ML model and in turn the AI-driven systems. This could have implications for industries that rely on AI, including healthcare, finance, and law enforcement.

In many cases public interest may outweigh individual's right to be forgotten. If a public figure, politician or a candidate to elections requests the removal of some information about him from the internet and such information is related to some crime or offence committed by him in the past then here the public's right to access takes prominence. In *Karthick Theodore vs. The Registrar General, Madras HC, IKanoon Software Development Private Limited, and Ors* CJI stated that "once a judgement is delivered it is a part of public record"

While at present steps are taken by the courts to redact and mask the names of victims of sexual crimes, no initiative is taken for individuals acquitted of crimes. The stigma of past accusations remains even if the person is proven innocent hindering in their efforts to rehabilitation, employment housing and social acceptance. The Right to be Forgotten has ethical concerns, it can help protect individual's life the same time it may also allow serious offenders to continue with their past actions, potentially putting the society at risk.

**Conclusion**
The right to be forgotten plays a crucial role in protecting an individual's privacy, enabling personal redemption. However, its application must be approached with caution as it has the potential to hamper public interest, technological progress, or societal accountability. Only through a balanced approach can Right to be Forgotten, be able to fulfil its intended purpose.

## NEWS CORNER

### *Cabinet approves guidelines for effective response to Cyber threats in Kerala State*

The Cabinet approved the Kerala Sectoral Cyber Crisis Management Plan, a detailed set of guidelines on cyber security in the Kerala State. The comprehensive crisis management plan will coordinate effective and quick response to cyber crisis and recovery from it. The Cabinet on Wednesday approved the Kerala Sectoral Cyber Crisis Management Plan, a detailed set of guidelines on cyber security in the State.
A crisis management committee chaired by the Chief Secretary has been formed as part of the guidelines.
The comprehensive crisis management plan will coordinate effective and quick response to cyber crisis and recovery from it.
The severity of cyber crisis, policies, damage to government institutions from a cyber crisis, responsibilities of government departments, coordination between stakeholders in case of a cyber attack have been covered in the plan.

It will be revised periodically depending upon the new cyber security threats, developing technology and new critical information infrastructure. The cyber crisis management plan has been developed on the basis of the Union Ministry of Electronics and Information Technology's cyber crisis management plan. A chief information security officer has been appointed in all major department for departmental coordination

## LATEST HIGHLIGHT

### *Digital Personal Data Protection Rules*

**The Digital Personal Data Protection (DPDP) Rules, 2025,** established by the Indian government, provide a legal framework for the processing, storage, and handling of personal data. These rules are a key step in implementing India's **Digital Personal Data Protection Act (DPDPA), 2023**. Released by the Ministry of Electronics and Information Technology (MeitY), India on January 3, 2025, the draft rules were open for public consultation until February 18, 2025.

The DPDP Rules 2025 outlines clear guidelines for businesses to follow in order to protect personal data and individuals' privacy. They empower citizens to have greater control over their personal data, requiring organizations to be more transparent, accountable, and responsible in their data practices.

**Key Provisions of the DPDP Rules**

The DPDP Rules, 2024, elaborate on various aspects of the DPDP Act, providing clarity and guidance on their implementation. Some of the key provisions include:

**1.Notice Requirements:** Data Fiduciaries (akin to data controllers under GDPR) are required to provide clear and easily understandable notices to data principals, specifying the types of personal data being processed, the purposes for which it is being processed, and how data principals can exercise their rights. These notices must be presented in an accessible and comprehensible manner, avoiding the common practice of burying essential details within lengthy and complex Terms and Conditions documents. Additionally, the notice must provide a communication link of the Data Fiduciary's website or app, and describe other methods (if applicable) for the Data Principal to withdraw consent easily as comparable to the process of giving consent, exercise their rights and make complaints with the Board

**2.Consent Management:** The rules specify the registration and obligations of Consent Managers, who act as intermediaries to facilitate the management of consent for data processing. Consent managers enable data principals to seamlessly provide consent for data sharing with data fiduciaries and facilitate data portability between them. Consent Manager must be a company incorporated in India with sound financial and operational capacity, having a minimum net worth of two crore rupees. The application for registration is to be made to the Board. The Consent Manager is also required to implement strong security measures to protect personal data, avoid conflicts of interest, and ensure transparency by publishing key management details and ownership structures.

**3.Data Principal Rights:** The DPDP Act grants data principals several important rights, including the right to access and correct their personal data, the right to erasure (also known as the right to be forgotten), the right to nominate another individual to exercise their rights in case of incapacity or death, and the right to grievance redressal. Businesses must establish processes and timelines for users to exercise these rights.

**4.Cross-Border Data Transfers:** The DPDP Act permits the transfer of personal data outside India, except to countries specifically blacklisted by the Indian government. The government has the authority to impose restrictions or requirements on data transfers to foreign states to protect the interests of Indian citizens. Security Safeguards: Data Fiduciaries are required to implement reasonable security safeguards to prevent data breaches, including measures such as encryption, obfuscation, or masking of personal data. They must also control access to computer resources, maintain logs to detect unauthorized access, and have measures in place for continued processing in the event of a data breach.

**5. Processing for provision or issue of services by the State or its instrumentality**: The State and its instrumentalities may process the personal data of Data Principals to provide or issue subsidies, benefits, services, certificates, licenses, or permits, as defined under law or policy or using public funds. Processing in these cases must adhere to the specific standards outlined in Schedule II, which ensures lawful, transparent, and secure handling of personal data for such purposes. The responsible parties must be accountable for adhering to these standards. The aim is to ensure that personal data processing is transparent, secure, and in line with legal and policy standards, safeguarding the interests of the Data Principals.

**6. Reasonable security safeguards:** A Data Fiduciary must implement reasonable security measures to protect personal data, including encryption, access control, monitoring for unauthorized access, and data backups etc. These safeguards ensure the confidentiality, integrity, and availability of data, and must include provisions for detecting and addressing breaches and maintenance of logs. Contracts with Data Processors must also ensure security measures are in place. The measures should comply with technical and organizational standards to prevent data breaches.

**7. Intimation of Personal Data Breach:** When a Data Fiduciary becomes aware of a personal data breach, it is required to promptly notify all affected Data Principals. This notification must be clear and straightforward, explaining the breach's nature, extent, and timing, along with potential consequences for the affected individuals. The Data Fiduciary must also inform the Data Principal of any measures taken to mitigate the risks and provide safety recommendations for protecting their data. Furthermore, contact information of a responsible person for inquiries must be included. Additionally, the Data Fiduciary must inform the Board Within 72 hours or a longer time if permitted, the Data Fiduciary is obligated to provide detailed information, including the events that led to the breach, actions taken to mitigate risks, and the identity of the individual responsible, if known.

**8. Time period for specified purpose to be deemed as no longer being served:** Under this provision, if a Data Fiduciary processes personal data for purposes outlined in Schedule III and the Data Principal does not engage with the Fiduciary within a specified period, the personal data must be erased unless required for legal compliance. This rule provides a clear process for erasing personal data if the Data Principal has not interacted with the Data Fiduciary within the specified time, ensuring that data is retained only when necessary for continued use or legal obligations, while offering the Data Principal a chance to retain their data by taking proactive steps

**9. Contact information for addressing data processing queries:** This mandates that every Data Fiduciary must clearly display on their website or app the contact details of a designated person who can address questions regarding the processing of personal data. If applicable, this could be the Data Protection Officer (DPO). The contact information should be easily accessible and visible to Data Principals, enable that they can reach out with any concerns or queries about how their personal data is being processed. The intent of this provision is to ensure transparency and accountability in data processing practices of Data Fiduciaries, by providing clear contact information, easier access to Data Principals to inquire about their personal data and its processing.

**10. Verifiable consent for processing personal data of children and persons with disabilities:** This provision outlines the requirements for obtaining verifiable consent from parents or legal guardians before processing the personal data of children or persons with disabilities. Specifically, a Data Fiduciary must implement measures to ensure that the person providing consent for a child's data processing is the child's parent or legal guardian, and that the parent or guardian is identifiable. For a child, the Data Fiduciary must verify that the parent is an adult by using reliable identity details or a virtual token mapped to such details. This verification process is critical to ensure that consent is being given by a responsible adult, in compliance with relevant laws.

**11. Exemptions from obligations in processing personal data of children:** This provision outlines certain exemptions to the standard requirements for processing the personal data of children These exemptions are applicable to specific types of Data Fiduciaries and for certain purposes, subject to conditions laid out in Schedule IV. According to Part A of the schedule, certain classes of Data Fiduciaries, such as healthcare professionals, educational institutions, and childcare providers, are exempt from specific provisions related to children's data. The processing of children's personal data by these entities is permitted, but it is restricted to specific activities like health services, educational activities, safety monitoring, and transportation tracking.

**12. Additional obligations of Significant Data Fiduciaries:** This provision brings specific responsibilities for Significant Data Fiduciaries. It mandates that these Fiduciaries must conduct a Data Protection Impact Assessment (DPIA) and a comprehensive audit once every year. The results of these assessments and audits must be reported to the Board, which need to contain key findings related to their adherence to data protection requirements.

**13. Rights of Data Principals:** Data Fiduciaries and Consent Managers must clearly publish on their website or app the process by which Data Principals can exercise their rights under the Act, including identifying details like usernames to facilitate identification. Data Principals can request to access and erase their personal data by contacting the Data Fiduciary. A Data Fiduciary must also provide clear timelines for responding grievances, ensuring an effective process with the necessary technical and organizational safeguards. Data Principals may nominate one or more individuals to exercise their rights under the law, following the procedures set by the Data Fiduciary and applicable legal norms.

**14. Processing of personal data outside India:** Data Fiduciaries processing data within India or in connection with offering goods or services to Data Principals from outside India must comply with any requirements the Central Government sets in respect of making such personal data available to a foreign State or its entities. This is intended to ensure that personal data remains protected under the Act.

**15. Exemption from Act for research, archiving, or statistical purposes:** The Act does not apply to the processing of personal data carried out for research, archiving, or statistical purposes if it adheres to the specific standards outlined in Schedule II. This exemption ensures that necessary data processing for academic and policy research can occur while maintaining certain safeguards and standards to protect personal data.

**16. Appointment of Chairperson and other Members:** A Search-cum-Selection Committee shall be formed by the Central Government to recommend candidates for the position of Chairperson of the Data Protection Board. The committee will be led by the Cabinet Secretary, Secretary MeitY, Secretary DLA and include two subject matter experts. Disclaimer: The purpose of this explanatory note is only to make it easier to understand the provisions of the Rules.

.....to be continued in the next edition of this Newsletter

# GLOSSARY OF TERMS
## Commonly used Terminologies in Cyber Crime Cases

**Cyber Grooming**

Cyber grooming is the process where an individual, often an adult, builds an emotional connection with a child or vulnerable person online to manipulate, exploit, or abuse them. This can involve deceptive tactics such as gaining trust through social media, chat rooms, or gaming platforms, with the ultimate aim of engaging in inappropriate conversations, soliciting personal information, or even arranging real-life meetings for malicious intent.

**Cyber Bullying**

Cyberbullying is the act of using digital platforms, such as social media, messaging apps, gaming forums, or emails, to harass, threaten, embarrass, or intimidate individuals. It can take various forms, including spreading false information, posting hurtful comments, sharing private or offensive content without consent, or engaging in online threats.

**Cyber Stalking**

Cyberstalking is the repeated use of digital communication tools, such as social media, emails, messaging apps, or other online platforms, to harass, intimidate, or threaten an individual. It often involves tracking a person's online activity, sending unwanted messages, spreading false information, or even attempting to control or manipulate the victim.

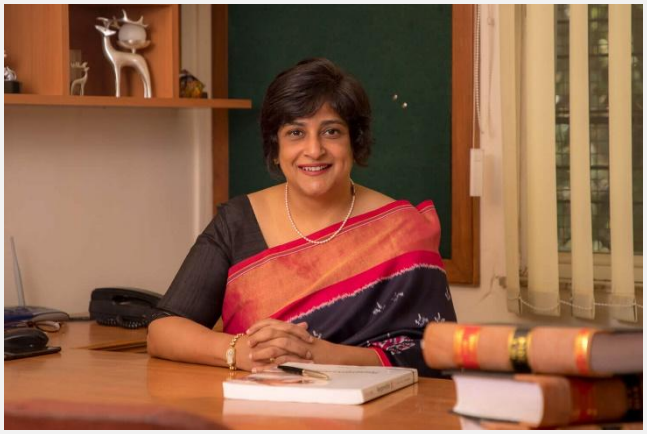
**Voyeurism**

Voyeurism is the act of secretly observing or recording someone, typically in a private setting, without their consent for personal gratification. This includes spying on individuals in places where they expect privacy, such as bathrooms, bedrooms, or changing rooms.

**Child Sexual Abuse Material (CSAM)**

Child Sexual Abuse Material" (CSAM) means any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer generated image indistinguishable from an actual child and image created, adapted, or modified, but appear to depict a child

# ABOUT THE AUTHORS



## Adv Vaishali Bhagwat

Vaishali Bhagwat is a practicing lawyer with 25 years of experience in civil and cyber litigation and advisory practice in Pune and Mumbai.
Vaishali has a prior degree and work experience in the field of Computer Science, a Post graduation certification in Cyber Security and Information Assurance and is a certified Privacy Lead Assessor.

She is an advisor to several companies on Cyber law and privacy compliance and advisor to various educational institutions on Protection of children from sexual offences.

She has successfully conducted several prominent cases for corporate espionage and Data theft, Data Privacy, Digital Financial Frauds, Cyber-crimes against women and children, take down orders and IP infringement in cyberspace.

Vaishali is a *TCS Chevening Scholar on "Cyber Policy and Cyber Defense" and has earned the Post Graduate certification from Cranfield University UK. She is also a Disha Alumni which is a prestigious program of the British high Commission on Innovative Leadership chaired by UK PM David Cameron and PM Manmohan Singh.*

www.vaishalibhagwat.com

**Mrudula Arjunwadkar**
*BSc., LLB, MPM*

**POSH Consultant**
Helping organizations in end to end POSH Compliance, External member to IC, POSH trainings

**Anagha Nair**
*BBA, LLB*

Intern, At V.P. Shintre and Associates

**Adv. Shyamal Marathe**
*MSc. (Electronics Sc), LLB, Certified Marriage Counsellor*

Engaged in training students of 11th, 12th 1st year engineering in Math and Physics subjects.
Head of Institute Centre for Excellence since last 10 years in Pune training students for IITJEE, IISER, CET entrance exams in Math and Physics and Electronics science