*Page: 582-600* *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

# LawFoyer International Journal of Doctrinal Legal Research

**[ISSN: 2583-7753]**

**Volume 4 | Issue 2**

**2026**

*DOI: https://doi.org/10.70183/lijdlr.2026.v04.175*

# CYBER RISK ASSOCIATED WITH QR CODES AND THEIR REGULATION IN INDIA

**Akshaya A**[1]

## I. ABSTRACT

*QR code (Quick response codes) are one of the major digital transformations in India. Several countries around the world have adopted QR code for availing various digital services, most especially for mobile payments. Every digital development will definitely have risks or complications, threats and vulnerabilities. So, this paper evaluates whether there is sufficient legal framework for regulation of QR codes used in various sector in India such as banking/merchant payment, business, education, government services, web access etc. The widespread adoption of digital services for everyday transactions, without fully understanding of it's their implications raise concerns about potential future issues. Therefore, effective collaboration between the financial sector, especially the Reserve Bank of India, cyber security centres, e-governance regulatory bodies, and educational institutions is essential to ensure safe and secure digital access and transactions. Developing countries like India, must take proactive initiatives to strengthen rules and raise awareness about the appropriate usage of QR codes in this digital age. Sector specific regulations of QR code is developed primarily in the banking and financial sector, whereas in most other sectors QR codes are widely used but the regulatory framework remains largely silent. Technical enhancement to a QR code should also ensure its reliability and functionality. AI based scams and other advanced risk are often closely associated with the rapid growth of emerging technologies. So, law should always be ready to prevent or curb the risk out of these emerging digital technologies. The increasing us of QR codes raises significant concerns on security and privacy. Mere awareness is not sufficient to address the risk arising from digital initiatives. A Combined approach of legal reforms and technical advancement is essential to mitigate this risk and to build to "Secure Digital India".*

## II. KEYWORDS

QR codes, cyber risk, transactions, malware, regulation.

[1] LLM (Cyber Space Law and Justice), 1st Year, Student at School of Excellence in Law, The Tamil Nadu, Dr. Ambedkar Law University, Chennai (India). Email:Akshaya31478@Gmail.Com

 (ISSN: 2583-7753)

## III. INTRODUCTION

Cyber risk means any disruption or damage resulting from cyber-attack it may be financial loss, operational interruption, reputational harm. Cyber-attacks may include malware (ransomware, spyware) attack, credential phishing/social engineering, data privacy risks (deception), physical tampering and other financial scams. Heavy reliance on QR code-based payments act as a single point of vulnerability that can overload banking systems and amplify risks of fraud, system failure and liability for bank. Now a days QR codes are essential for navigation of any registrations via online, status tracking, making payments, government uses QR codes to facilitate access to its digital services. It enhances easy accessibility to reach out people's digital need easier than traditional operations. The vulnerability and risk associated with QR codes are uninformed and not addressed properly, the reason for such case is lack of sufficient regulations and specific forum in India.

QR codes have significantly contributed to India's digital transformation by making transactions simple and efficient. However, the risks associated with the use of QR code are not effectively regulated, they may undermine India's long-term development and erode public confidence in digital systems. In the long run, this could result in digital fatigue and reduced reliance on digital platforms. Cybercriminals often possess greater technical expertise than ordinary individuals and exploit this knowledge for their personal gain. Digital hygiene for the secure use of QR codes can be promoted through practices such as verifying the source, using trusted scanning applications, and avoiding suspicious links.

However, for an average user, it is often impractical to undertake detailed verification, especially since QR codes are primarily used for quick and convenient access. In this context, legislation, governance policies, and regulatory directions issued by various sectors play a vital role in establishing and enforcing best practices for the safe use of QR codes in India.

"The speed and convenience of instant access are often balanced by corresponding risks and responsibilities."

 (ISSN: 2583-7753)

### A. Statement Of the Problem

Cyber risk pertaining to QR Codes are still underexplored in India, since this will lead to gradual and potentially less noticeable effects that may become apparent over a time. So, the regulations pertaining to these threats in various sectors which is dominant in use of QR codes are to be reconsidered and needs to be implement in a better way for prevention of such vulnerable situations. Regulatory guidelines are not enough to tackle these cyber threats committing through QR codes, applicability of legal provisions needs to be strengthened to ensure cybersecurity protection.

### B. Research Objectives

The main objective of this research is to mitigate or to prevent misuse of QR code technology in this digital era. Strict regulations ensure digital hygiene to make avail all form of digital services in secured way. Technology and innovation both jointly lead the current and future generations, so bringing them under an umbrella of laws and rules will safeguard progress towards a digital India.

### C. Review of Literature

A study by Avinash Ashokrao Kolte (2023) regarding a general overview on QR code awareness in India and discussed where it improves country's digital economy. The key focus of the study is transition of digital payments after demonetization in India. QR codes facilitated for payment system for making contactless payments especially during Covid pandemic. With relevant to regulation, RBI is governing body and thus it regulates such payment system. Other than payments QR code also plays crucial role in agricultural development, education, consumer awareness and healthcare for easy access of information. The paper also discussed the challenges pertaining to QR codes such as security risk, privacy concerns, lack of user awareness. Overall, the existing literature concludes that QR code have contributed to digital transformation, where its effective utilization depends on user education, ensuring security and advancing technological infrastructure.

In recent study made by Mohanraj.S and Pradeep.G (2026) analysed on adoption trends and security challenges of QR codes in India. QR codes are nowadays used in major digital ecosystem such as in banking, retail, healthcare, public administration,

education due to ease of use and compatibility. This paper identifies major cyber threats such as QR phishing, malicious redirection, malware attacks, unauthorized data access and leakage, payment scams through QR code manipulation. The study emphasizes that QR code act as "black box" where users can't verify the digital content inside it, so it may cause various cyber threats. The literature quoted that there were constraints of use of static QR code architecture in India. They lack security features such as encryption, authentication, expiry mechanism, and validation. Another finding is lack of digital literacy and user awareness. The study finally suggested a secure dynamic QR code framework which is integrated with encryption payloads, digital signatures, domain verification and fixed term validity.

Existing literature by Harikrishnan S (2026) involving OTPs and QR code scanning in cybercrime focused on legal challenges and emerging responses in India. Most cybercrimes rely on social engineering techniques. QR code related fraud indicate that there is lack of transparency and verifiability makes suspectable to misuse. The paper discussed that there is inadequacy of existing legal framework for dealing authentication-based cybercrimes. Statutes such as the Information Technology Act, 2000 provide a foundational legal framework for addressing cybercrime; however, they do not specifically deal with emerging threats such as OTP fraud and QR code misuse.

### D. Research Gap

Existing research has largely focused on providing a general overview of QR code technology, including awareness, adoption, benefits, and challenges such as privacy and security concerns. Most prior studies have concentrated on the use of QR codes in the banking and digital payment sectors. However, the role of Reserve Bank of India (RBI) in addressing and regulating crises arising from QR code misuse remains underexplored. Although technical vulnerabilities associated with QR codes have been widely discussed, limited attention has been given to the adequacy and effectiveness of the existing legal and regulatory framework. Consequently, there is a clear research gap in integrating cyber risks with legal and regulatory analysis, particularly in the Indian context. This paper seeks to bridge that gap by examining

the risks associated with QR codes and evaluating the legal framework governing their use in India.

### E. Research Methodology

This paper has adopted doctrinal research methodology to analysis the legal frameworks in protection of QR code-based risk and threats in India. The primary and secondary sources relied upon legislative instruments, NPCI and RBI circulars, judicial decisions and academic literature. The paper discussed sector-based approach how QR has been used in various discipline and in what way it creates risk in those sectors. To evaluate how the sector-based regulations give guidelines specifically for mitigating the risk prevailing in those sectors. The Article has a major limitation stating that the paper stands remain only a doctrinal approach when examining a rapidly evolving technical and regulatory landscape.

### F. Research Questions

1. What is the risk prevailing in QR codes?
2. What are the sectors which adopts QR code?
3. Whether there is any law or regulation which governs QR code in India?
4. How does India mitigate threats out of QR codes?

### G. Research Hypotheses

**1.** The existing legal framework in India is inadequate to regulate and prevent QR based risks in different sectors.

**2.** The current legal framework in India is sufficient to regulate and prevent QR based risks in different sectors.

## IV. RESEARCH AND ANALYSIS

### A. Use Of QR Codes and Its Challenges

QR Codes are of two types, Static and Dynamic. Static Codes have fixed information that cannot be altered after creation whereas a dynamic QR code stores a short URL that directs to actual content which can be altered or changed at any time. QR codes are two-dimensional barcode made up of black and white squares that stores more information than an actual traditional barcodes.

### 1. QR codes in Banking and Financial Sector

QR Codes increases a massive transaction via UPI payments. It enables a merchant payment, bill payments etc. In financial sector QR codes are incorporated mainly for faster, convenient and paperless transactions. The UPI based QR codes rose from 24.42 crore in 2023 to 73.84 crore in 2026 where this shift towards QR code shows how it plays role in current digital transformation.[2] On April 2016, the Unified Payments Interface (UPI) was launched by the National Payments Corporation of India under the framework of the Payment and Settlement Systems Act, 2007. India's interoperable Bharat QR was introduced in 2017 and supports major card networks including Visa, Mastercard, RuPay and American Express. Its launch was guided by the Reserve Bank of India's earlier Payments Vision 2018, which promoted interoperable and low-cost digital payment infrastructure. At present, the regulatory and policy framework is governed by the RBI's Payments Vision 2025, which focuses on "E-Payments for Everyone, Everywhere, Every Time" and emphasizes fraud prevention, secure QR-code-based payments, and stronger authentication mechanisms to enhance trust in the digital payments ecosystem.

### 2. Replacement of QR codes

As discussed above QR codes are of two types. Fake QR codes are replaced for original codes for making the payment in static code. Money goes to fraudsters instead of merchant's account. Dynamic QR codes will have pre-filled transaction details where it is considered to be little safe than static when properly implemented. Static QR code scam is usually a physical tampering whereas in dynamic QR code, there will be a redirection to a malicious links or phishing attacks and data privacy concern. To avoid scam over static QR codes there is a "sound box" which acknowledge the merchant and buyer through audio announcement features. It ensures confirmation of payment, and easy for the merchant to track payment to check whether the correct amount has been paid.

### 3. Quishing

[2] Vismay Basu, Shifting Patterns of Paying Instruments, The Indian Express,25th Feb 2026.

Phishing through QR codes ("Quishing") is an emerging cyber threat in which fraudsters circulate malicious QR codes through e-mails, messages, or social media while impersonating legitimate banks or financial institutions in order to deceive users into disclosing confidential information or downloading malware. The act of impersonating a genuine entity and inducing the victim to act is primarily punishable under Section 66D of the Information Technology Act, 2000, which penalizes cheating by personation through the use of a computer resource.

Where the credentials or other unique identification features obtained through such deception are subsequently used fraudulently, Section 66C of the Act, relating to identity theft, also becomes applicable.[3] It is a social engineering technique used by scammers to track the vulnerable by providing personal or sensitive information or downloading malware onto the device.[4] Regulators are facilitating the use of digital techniques and thus circular from NPCI stating that rules for offline QR codes should follow UPI brand guidelines and should display UPI logo. Before incorporating new QR designs there should be a prior approval from NPCI.[5]

NPCI has taken steps in protecting secured transactions by eliminating international QR share and Pay (P2M) which means scanning a QR code which is sent through WhatsApp or image for receiving payment from other countries were scanning a QR code in physical stores in other countries are allowed. It may reduce QR tampering, Quishing and other cross border fraud payments.

### 4. QR codes used for credit money scams

In a "scan to receive money" fraud, the perpetrator falsely represents that scanning a QR code is necessary to receive funds into a bank account, even though money can be credited directly through the recipient's UPI ID or registered mobile number. Acting under this misrepresentation, the victim voluntarily authorizes a payment to the fraudster through the Unified Payments Interface (UPI) operated by the National Payments Corporation of India (NPCI), resulting in unauthorized financial loss. Such

[3] Sec 66C of Information Technology Act,2000
[4]Australian Cyber Security Centre, Quishing | Cyber.gov.au (Mar 29,2026) 17.26
[5] NPCI/UPI/OC no. 190/2023-24 Reiteration of Compliance of Certain NPCI Circulars.pdf

conduct constitutes cheating and is punishable under Section 318 of the Bharatiya Nyaya Sanhita, 2023.

### B. QR codes in government services

QR codes are part of e-governance, it is overseen by Ministry of Electronics and Information Technology and RBI for payment system. Now a days government bills, e-tickets and payments are paid using QR code, it is a modern way of public services. It connects web resources with physical places where it bridges a gap between offline and online services.

#### 1. Privacy Issue

Government has all records and data of its citizen through authenticated ID card called Aadhar card initiated by Government of India. Earlier version of Aadhar has only demographic information of the holder there is no strong encryption technology but there is a new initiative called secure QR Code which is a visual code contains demographics and photograph of the Aadhar number holder which is digitally signed by UIDAI[6]. This ensures if any fraud attempted on Aadhar can be easily detected by using this QR code scanner. This QR code contains data such as Ref ID, Name, Gender, DOB, Mobile, Email, Address, Photo and 2048-bit digital signature. This verification depends on UIDAI's official scanner application, and it can be scanned without internet, yet it is not adopted widely. If there is any tampering of data, it can be easily detectable.

Although QR-based verification is often regarded as a tamper-resistant mechanism, it raises significant privacy concerns. The primary risks include unauthorized access to personal data and the absence of consent-based access controls. Unlike One-Time Password (OTP)-based authentication, QR code verification may not require real-time user approval at the moment of scanning, thereby increasing the possibility of misuse and unauthorized data access. To curb this privacy issues there should be a dynamic and revocable QR codes as a valid mode of identity verification. So, law should mandate time-bound validity or expiry features and consent-based access. Only

[6] Unique Identification Authority of India, GOI QR Code Reader - Unique Identification Authority of India | Government of India Mar 30,2026 (1.12pm)

licensed entities can scan and access the data inside the QR code, and it should ensure that it is done with official UIDAI verification systems. Aadhar has been already poses a several privacy concerns, court have already ruled that right to privacy is a fundamental right under constitution of India[7]. Same way as Digi locker initiate under digital India, where documents and data stored are secured and protected but there is insufficient regulation of access and sharing through QR codes.

**2. QR codes in GST e-invoice**

Under CGST Rules, 2017[8] a tax invoice contains QR code with embedded Invoice Reference Number (IRN) in E-invoice. This enables authentication and verification of invoices; this helps in preventing tax evasion and fake invoicing. QR codes in GST are regulated and secured which is IRN based and dynamic QR codes, but fake E-invoice may be filed for claiming Input Tax credit from government, So the QR codes generated under IRN is technically secured but how it is used or misused in practice usually buyer does not scan the receipt. There is no strict obligation or enforcement to verify such QR codes.

**3. Placing Fake QR code**

Scammers place bogus QR codes near ticket counters, parking payment gateways, transport entry points. This led to direction for fake bookings or payments. It exploits public infrastructure. There is no official QR codes for availing such services thus creating entirely new fraudulent QR codes. The same incident happened in Pune, cybercrime officials warned to avoid use of unofficial roadside QR codes.

**4. Malware and ransomware attacks through QR codes**

Security risk associated with QR codes only drive from destination not from the code itself. If any QR code which redirects to malicious site where malware gets installed. It steals contact details, messages and other credentials. Same way ransomware attack happens which redirects to malicious APK or file where it locks a device or encrypts data and demand payment. It is an offence punishable under IT act and BNS. To prevent such cyber threats regulations, needs to be framed to control over QR linked downloads and there is need of authentication mechanism for such redirections.

[7] Justice K.S. puttaswamy v. Union of India WP (C) 494/2012
[8] Rule 46 &48(4) Central Goods and Services Tax

Ensure integrated responsibility on service providers, platform operator and public authorities.

### C. QR codes in commercial and business sectors

QR codes facilitate easy trade flow it is used in payment system, packaging, product promotion etc. This plays a major role in different commercial relationship such as B2B, C2B and B2C. But there is no uniform security mechanism for above all models. RBI has permitted to use UPI and Bharat QR code for payment system used in business and commercial establishments. QR codes are also used in accessing product information, making feedback by consumers. Risk pertaining to payment related scam are already discussed the same above in banking sector, whereas others are as follows:

1. **Malicious QR payload attack or QR-based Remote Code Execution (RCE):** Payload is an actual content inside the QR code. In malicious context, it harms user or system. This QR code contains fake website, download link for malware, target bugs to access camera, storage. It is also used for data or credential theft. It contains harmful instruction and deceives and exploit the user and there is vulnerability in software. It is very dangerous than all other cyber threats it involves spy on user, data theft, control of device and networks, install malware or ransomware, it bypasses the user control. These threats are usually done by cyber criminals who are well equipped in technical knowledge.
2. **QR Brushing scam:** While receiving unsolicited packages containing a QR code which contains malicious sites, phishing pages which may cause data stealing, identity theft and financial loss or may be in surveillance. These scans are done by seller. In 2022 there was an amendment to Legal Metrology (Packaged Commodities) Rules, 2011 which regulated labelling of packaged products through QR codes. This amendment is bought by Department of Consumer Affairs (DCA) to disclosure of product information in detail via QR codes and other basic details of the product can be displayed through physical disclosure. This is only a digital approach and not full-fledged regulatory framework. If QR codes become error or

fails to scan, redirect to some other sites there is no consumer protection mechanism for this digital disclosure.

### D. IPR in QR codes

QR code is a registered trademark owned by Denso Wave Incorporated, this right has been declared worldwide but it is not enforced. The code has been standardized in accordance with ISO/IEC 18004.It was invented by Masahiro Hara in the year 1994 in Toyota's subsidiary company for tracking automobile parts.

QR codes are integral part of retail, logistics, business etc. Intellectual property rights protection over such use of QR codes in business and commercial sectors needs to be understood through the legal position of such intangible rights. Copyright protection cannot be given to QR codes as it falls under functional and factual tool but the encoded data or content, audio inside the code can be inclusive of existing copyright laws. When it comes to trademark protection brand logo embedded in QR codes and used as source identifier can claim its protection example QR Code Monkey it is a brand owned by Berlin company where this platform engaging in generating custom QR codes.

Patent protection pertaining to QR codes will be in the form of encoding algorithms, any security enhancement techniques when there is added innovation to existing code. Denso Wave holds its patent right where it is generated under ISO/IEC 18004 technology which provides open access to use freely and publicly. So, these protections are not absolute, but it gives indirect approach to get legal protection, thus QR codes are not creative they are just a functional tool in digital eco-system. These IPR in QR code raise complex subject without proper regulatory mechanism.

In Niranjan Arvind Gosavi v. Innovatiview India pvt ltd[9], this is the first case which the court dealt patent dispute and observed that QR code / machine readable bar code authentication system technology, where the plaintiff alleged infringement in a "e-tender for QR Code solution with encoded texts" issued by National testing Agency for enhanced QR-code solutions could only be implemented using patented method

[9] Niranjan Arvind Gosavi and Ors v. Innovatiview India Private Limited,CS(COMM) 214/2024 (Delhi High Court,13 March 2024).

and therefore, the defendant's participation in the tender itself amounted to patent infringement.The court considered defence under section 47 of the Patents Act which permits government or its authorized agents to use a patented invention for its own purposes without constituting infringment and refused interim injunction noted that any such order could distrupt a nationwide pubic examination system.At the same time the court protected the plaintiff's interest by directing the defendant to maintain accounts of revenue, thereby balancing private patent rights with public interest.

This case is significant as it highlights the complication in enforcing patent rights in emerging digital technologies like QR code systems, particularly when such technologies are used in government functions and demonstrates the judicial approach while granting relief by considering larger public implications.

## V. LEGAL AND REGULATORY OVERSIGHT

There is no separate provision or specific law governing to tackle risk related to QR code. Motive behind QR code risk is for data theft, inserting malware, direct to malicious sites, financial scam and other concern is privacy.

Above motive create opportunities for cyber criminals to accomplish using various techniques to commit different offence such as QR quishing, code tampering, fraudulent redirection etc.

### A. Regulatory Frameworks Regarding QR Codes

In 2020 RBI issued circular regarding digital payment transactions particularly on QR code infrastructure to operate interoperable QR code such as UPI and Bharat QR codes to remove card swiping machines and facilitates multiple payments through one code. It is considered as standardized QR codes for payment system in India. This measure has taken under section 10(2) and 18 of Payment and settlements Act, 2007[10].

Recently NPCI has halted the concept called QR share and pay for cross-border payments to curtail the QR related scams.

QR code-related fraud is addressed under the Information Technology Act, 2000, particularly through Sections 43, 66, 66C and 66D. Section 66D is the principal

[10] Reserve Bank of India RBI/2020-21/59 DPSS.CO. PD. No.497/02.14.003/2020-21 www.rbi.org.in

provision applicable to most QR-based scams. It punishes cheating by personation through the use of a computer resource or communication device with imprisonment of up to three years and fine up to one lakh rupees. This provision directly applies to quishing, fake merchant QR codes, fraudulent "scan to receive money" schemes, and other scams in which the offender impersonates a bank, merchant, service provider or government authority to deceive users into making payments or disclosing credentials. Where the credentials or unique identification features obtained through such deception are subsequently used fraudulently, Section 66C relating to identity theft is also attracted. Thus, Sections 66D and 66C operate complementarily, with Section 66D addressing the initial act of deception and Section 66C addressing the later misuse of the victim's credentials.[11]

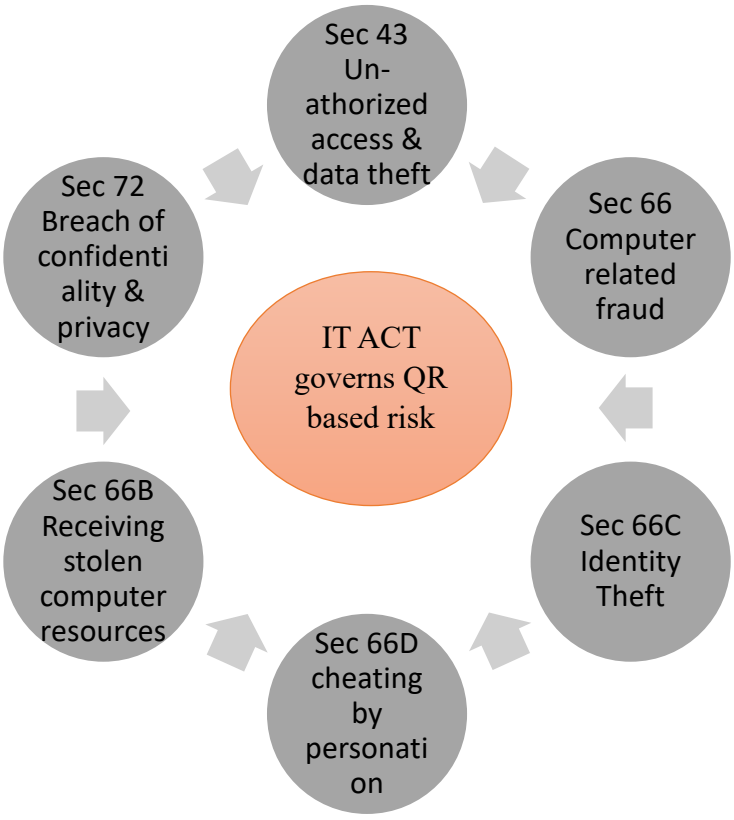


*Figure 1*

[11] Sec 43,66,66C,66D,66B,66E,72

Law does not define what is QR fraud or scam and the laws and regulations are fragmented and indirect based on different sectors. Risk arises from both physical misuse and technical or software level.

The Consumer Protection Act, 2019 is also relevant where QR codes are used in commercial transactions and consumers are deceived through fake merchant QR codes, brushing scams, or misleading redirections. Section 2(47) defines "unfair trade practice" to include deceptive or misleading representations that cause consumer loss. A trader or platform that displays false QR codes, conceals material information, or redirects consumers to fraudulent interfaces may attract liability under this provision. Section 18 empowers the Central Consumer Protection Authority (CCPA) to protect consumer rights and to investigate, recall goods or services, discontinue unfair practices, and issue directions against misleading digital conduct.

In addition, the Consumer Protection (E-Commerce) Rules, 2020 require e-commerce entities to provide transparent and accurate information regarding sellers, grievance mechanisms, and transaction details. Where QR codes are used to facilitate purchases, payments, or access to product information, these provisions strengthen consumer protection by addressing deceptive digital practices and ensuring accountability of businesses and online platforms. The Digital Personal Data Protection Act (DPDPA) 2023, read with the DPDP Rules, 2025, is directly applicable to QR code risk when a QR code is used for collecting personal data:

1. Applicability of Digital Personal Data Protection Act under section 3: If a QR code redirects to a site or app and collects personal data like name, phone number, bank details etc., then DPDP act applies immediately.
2. Section 6 requires the consent of the Data Principal for processing personal data, and such consent must be free, specific, informed, unconditional and unambiguous. The consent must relate to the purpose specified in the notice under Section 5 of the Act.
3. Data fiduciary must give clear notice before collecting personal data, it should state the specific lawful purpose of processing the personal data to Data Principal.

4. Under section 8, Data fiduciary must ensure accuracy of data, should take reasonable security measures and prevent to data breach. If the data has been breached it should be informed to the board called Data Protection Board of India.
5. Data Principal has right to information i.e user can ask what data has been collected and for why it has been collected, another right is for correction and erasure. These rights are not exercised against the QR code itself but against the Data fiduciary that collects and process personal data through the QR-enables interface, therefore their applicability depends on the existence of a legitimate data controller.
6. If personal data has been collected via insecure QR system or the data is leaked due to negligence, then there is monetary penalty upto Rs.250 crore and there will be a separate penalty for failure to notify the data breach. DPDP Act deals only with data protection and does not punish cyber criminals directly. The Act specifically states that data fiduciaries must provide a robust grievance redressal mechanism for data Principal.

Application of Bharatiya Nyaya Sanhita 2023 in QR code related scams with examples:

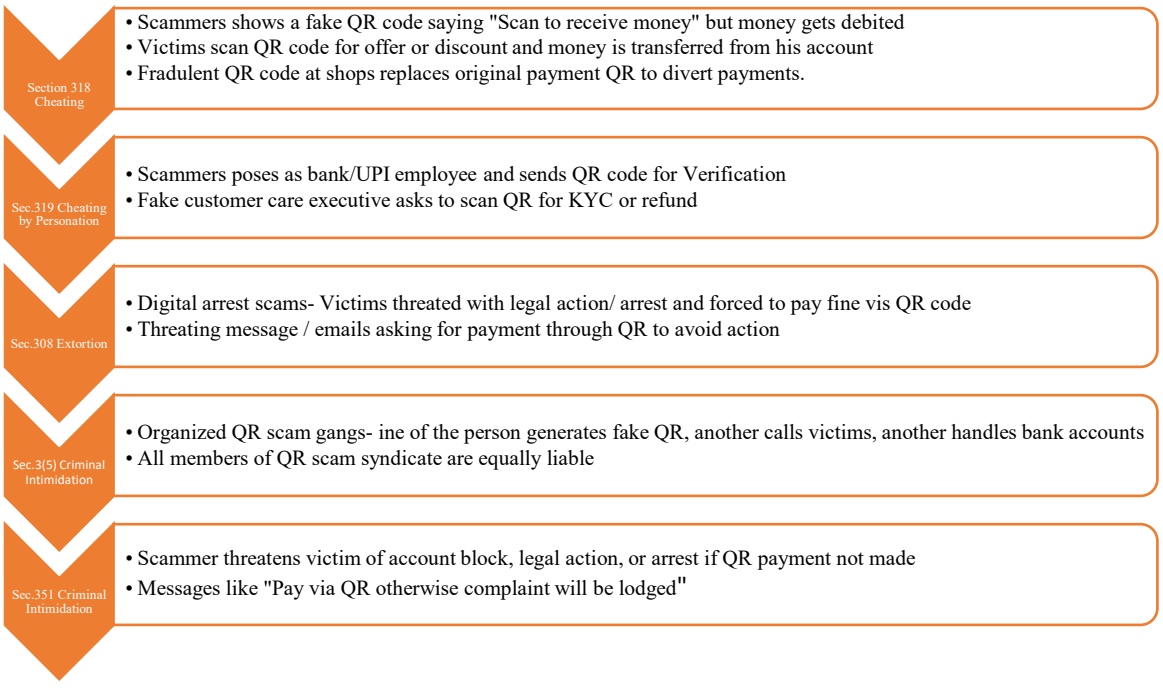


*Figure 2*

## VI. ROLE OF JUDICIARY ON QR CODE REGULATIONS

Digital transformation in judiciary is being implemented in both administrative and justice delivery system. QR codes are the key gateways for accessing information and status of tracking cases. E-courts in India has developed QR code-based services. Another initiative is QR code based digital entry pass system for entry and exit in courtrooms initiated by e-committee, Supreme court of India. Judiciary is not exempted in use of QR codes but focusing on best practices on use of QR code to mitigate risk is to be addressed.

Apoorvanand jha v. Union of India[12], in this case the court ruled that during kanwar yatra in 2025 specifically Uttar Pradesh and Uttarakhand government ordered to display a QR code in hotels, food stalls to provide information on owner's name, staff details, registration and licence details and its menu. Controversial part of this digital disclosure via QR code is identity disclosure it indirectly reveals the caste and religion of the person. This issue has already dealt in 2024 where shops can display types of food and menu, it cannot be forced to reveal owner's name and other identity but now the same issue extending it to scan through QR code. This violates Right to equality under Article 14, freedom of business under Art 19(1)(g) and right to privacy (Art 21). Contentions given by government is where this ensures consumer awareness and pilgrims have dietary preferences, QR code improves transparency. The court did not hold the final verdict instead it ruled that yatra is ended and follow the existing law, it gives direction regarding disclosure of Licence and registration certificate. It doesn't either reject or approve the use of QR codes. This remains unresolved constitutional validity of digital tools like QR codes to be used for disclosing identity and concern on privacy related issues.

## VII. SUGGESTIONS TO MITIGATE RISK RELATED TO QR CODE

1. Major indirect legislations include the Information Technology Act, 2000, the Consumer Protection Act, 2019, and the Bharatiya Nyaya Sanhita, 2023. Together, these statutes address cyber fraud, unfair trade practices, and criminal

[12] Apoorvanand Jha & Anr v. Union of India, W.P (Crl.) No.328/2024 (Supreme Court of India, decided 22 July 2025).

liability arising from QR-code-based misuse. However, these sector-based regulations remain fragmented, and a specific statutory framework dealing exclusively with the generation, deployment, and misuse of QR codes would provide greater legal certainty and consumer protection. Now there is no regulation to generate QR codes anyone can make no mandate of licensing from any authority.

2. Digital signature based QR are only used in governmental portals it should be extended to other verifications process done by employment, business, banking etc.
3. For replacement of fake QR codes already there is soundbox but there should be mandatory display of verified merchant ID alongside in static QR codes.
4. There should strict adherence to interdiction of use of static QR codes for high value transactions. Limiting certain amount of threshold to be maintained and regulated.
5. Specific provision to penalize QR code-based offence such as unauthorized generation, alteration and substitution of fake codes. Need to amend Information Technology Act for mitigating this risk.
6. Other than banking sector, QR codes are to be regulated in government services such as railways, state transports, hospitals, government offices, education sectors etc and also in private entities.
7. Use of QR codes is huge and it has been implemented almost in all sectors, its efficiency and technical safeguards need to be improved in such way generating Expiring QR codes, one-time use QR, scan history logs, fraud detection mechanisms etc.

## VIII. CONCLUSION

Digitalisation without regulation often lead to risk complication. Same way expanding the use of QR codes in all sectors should be supported by proper regulation. Only advisories and best practices alone cannot create security over such risk. Wide usage of QR codes among general public is necessary to ensure that data conveyed is not harmful to its users. There are two major attacks such as attack on

human interaction and automated attacks.[13] Some of the innovations paves way towards India's digital infrastructure particularly through QR codes such as QR code based payments, Digital Malkana to track seized properties by court or police, QR codes linked to audio, geo-tagged QR codes which provide directions to identify locations and routes, Artistic QR codes by AI to promote brands, smart QR codes etc.

These innovations provide comprehensive development of digital access across country. In India regulatory such as RBI for using interoperable QR codes, Central Board of Indirect Taxes and Customs for use of dynamic QR code for B2C invoices with businesses turnover above Rs.500 crore. Innovations, Digitalization through adoption of QR codes in various sector in India has to be raised rapidly, future might be successful only when regulatory frameworks are capable to address risk associated with QR codes. Digital India is not only a shift towards electronic services and expanding all sectors into digital eco-system true success of digital transformation is addressing issues arising out of digital environment.

*"Technical Initiative will become systematic threat when it is implemented without regulations"*

## IX. REFERENCES

### A. Primary Source

1. Information Technology Act 2000
2. Bharatiya Nyaya Sanhita 2023
3. Digital Personal Data Protection Act 2023

### B. Secondary Source

1. https://www.npci.org.in/blog/qr-codes-the-new-age-tech-shaping-india-s-digital-payments-landscape

[13] CERT-in Advisory CIAD-2017-055 QR code Security Best Practices issued on Dec 7,2017 https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2017-0055 (Apr 03,2026)

2. https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2017-0055
3. 156-12-2021_20gst_20circular.pdf
4. QR Codes and Their Role in Legal Institutions - Leaders in Law
5. https://www.computer.org/publications/tech-news/trends/qr-code-risks
6. QR Code Reader - Unique Identification Authority of India | Government of India
7. https://www.researchgate.net/publication/318125149_An_Introduction_to_QR_Code_Technology
8. https://ieeexplore.ieee.org/document/7966807
9. https://www.google.com/amp/s/www.thehindu.com/education/qr-linked-textbooks-expand-access-but-struggle-to-sustain-engagement/article70792092.ece/amp/