

**USE OF DIGITALIZATION BY JUDICIAL, POLICE AND OTHER
AUTHORITIES TO PREVENT AND DEAL WITH CRIME BEFORE ARREST
AND AFTER ARREST AND ITS LEGAL RECOGNITION, PRACTICAL
ISSUES, AND CHALLENGES**

by

Dr. Teena Sundarbanshi

ABSTRACT

The world today is rapidly evolving across multiple dimensions, with traditional practices being swiftly replaced by technology. The internet and digital tools have transformed not only the way we think but also the sources from which we derive our thoughts, and the platforms we use to express them. In present times, the internet, computers, and applications like WhatsApp have become essential parts of human life. However, this transformation is not confined to individuals alone—it is also significantly impacting the legal system, including the execution of laws. Many times, judiciary and police are taking help of digital tools to deal with crimes to prevent it or cure it. Where they not only use digital tools to watch on criminals, to take their attendance but also use it to take access of websites, other apps so that further crime and other things can be prevented. This use of digitalisation has given birth to the One emerging concept that is "Digital arrest" which rampantly misused by the scammers and becomes a wake-up call for police, judiciary, and other legal authorities. Other than that, digital restrictions prior to arrest and after arrest raises many numerous legal, constitutional, and validity-related challenges since there are no specific laws on that which permits or denying the use of such digital restrictions after or prior to arrest. Therefore, through this research paper, the researcher aims to study the concept of digital restrictions, Digital arrest and its legal standing, its position within the framework of existing laws, related legal questions, the judiciary's perspective on the issue, the opportunities it creates for criminal misuse, and possible solutions to these challenges. However, the concept of digital restrictions raises several legal and practical concerns. Questions arise regarding the legal foundation of this practice: under which law does it operate, how is it implemented, and does it have formal legal recognition? Concerns also emerge about its impact on fundamental rights—if digital

restrictions infringe upon such rights, can their use still be justified? Furthermore, there are instances where fraudsters exploit public fear of such restrictions by impersonating police and other officials and falsely claiming to place victims under “digital arrest”, a practice that has no basis in law. This creates the need for clear mechanisms to identify, prevent, and punish such misuse.

Key words: Digital arrest and digital restrictions, Digital restriction, Law, Judiciary, Legal Validity, Technology, Challenges

Introduction

Maintaining law and order is a crucial part of the criminal justice system. This system employs several measures to establish peace in society, one of the most important being the arrest of individuals or the prevention of activities that may lead to crime. Through arrest, a suspect is taken into custody by the authorities to ensure that they do not disturb public peace, harm members of society, threaten witnesses, tamper with evidence, obstruct an ongoing investigation, or engage in activities that may further criminally acts. Similarly, preventive measures restrict individuals, on legally justified grounds, from engaging in conduct that could result in harm to society. Legal action against offenders—both to punish them and to deter future crimes—often serves as the basis for justifying an arrest.

With changing times and the growing influence of technology, many aspects of crime and its control have undergone significant transformation. The internet has not only altered the methods by which crimes are committed but has also reshaped their detection, investigation, and prevention. Technological advancement and digitalization have equipped offenders with new techniques to commit crimes, while simultaneously compelling the criminal justice system to adopt digital methods of crime control. The scale of this shift is visible in official data. According to the National Crime Records Bureau’s report Crime in India 2024, registered cybercrime cases rose by 17.9 per cent, from 86,420 in 2023 to 1,01,928 in 2024, even as overall cognisable crime fell by about 6 per cent, and fraud alone accounted for 72.6 per cent of these cybercrime cases.¹

Digital restrictions, and the use of technology by police and judicial authorities, have emerged as one such method in response to the growing impact of technology on crime and its

¹ Gautam Debroy, ‘NCRB Report Shows Sharp Rise in Cybercrime Despite Overall Decline in Crimes’ *ETV Bharat* (New Delhi, 7 May 2026) <<https://www.etvbharat.com/en/bharat/ncrb-report-shows-sharp-rise-in-cybercrime-despite-overall-decline-in-crimes-enn26050702556>> accessed 23 September 2026.

commission. This mechanism was specifically developed to address digital crimes and to prevent their occurrence by introducing measures tailored to technology-driven offences.

However, the concept of digital restrictions raises several legal and practical concerns. Questions arise regarding the legal foundation of this practice: under which law does it operate, how is it implemented, and does it have formal legal recognition? Concerns also emerge about its impact on fundamental rights—if digital restrictions infringe upon such rights, can their use still be justified? Furthermore, there are instances where fraudsters exploit public fear of such restrictions by impersonating police and other officials and falsely claiming to place victims under “digital arrest”, a practice that has no basis in law. This creates the need for clear mechanisms to identify, prevent, and punish such misuse.

Overall, this evolving practice presents multiple challenges that must be addressed to ensure that digital restrictions and digital arrests are applied in a legally sound, rights-respecting, and socially beneficial manner. Since the validity and recognition of these practices within existing legal frameworks are often questioned, it becomes essential to address these concerns and ensure that digital methods of crime prevention and investigation gain proper recognition under the law.

Meaning of Restrictions and its Traditional Methods

Restrictions in law refer to lawful limitations imposed on the enjoyment of rights, freedoms, or activities of individuals with the objective of maintaining public order, morality, security, and justice. They do not abolish rights but regulate them to ensure a balance between individual liberty and the larger interests of society. Traditionally, restrictions have been applied through legal and procedural mechanisms such as preventive detention, curfews, censorship, licensing, regulation of assemblies and processions, imposition of fines or penalties, and preventive measures under criminal law. These methods were primarily focused on controlling physical spaces, gatherings, and expressions that could disturb peace or threaten the State. Thus, traditional restrictions relied heavily on physical enforcement by police and judicial authorities to prevent crime and maintain law and order.

Overall, in law, the term *restriction* refers to a lawful limitation imposed on the exercise of a right, liberty, or activity for the larger benefit of society, public order, morality, security, or justice. Restrictions are not meant to abolish a right but to regulate its scope in a way that balances individual freedom with collective interests.²

² Article 22 Preventive Detention in Constitution of India, Section 41: Police may arrest without warrant in certain cases, Section 144 CrPC: Magistrate may impose restrictions (curfew, ban on assembly) to prevent obstruction,

Meaning & Procedure of Traditional Arrest

Arrest has not been precisely defined in law; however, its general meaning can be understood as the curtailment of a person's liberty. Every individual enjoys the fundamental right to life and personal freedom regarding his body, liberty of his thought, but the moment this freedom and liberty is restricted in accordance with the procedure established by law, it amounts to an arrest.³ In such a situation, the person's freedom is taken under the control of the State or its lawful authority. Consequently, the individual's body and mind come within the custody of the authority, and he ceases to remain free as per the procedure established by law.¹ While the Constitution, particularly Article 21, guarantees that no person shall be deprived of life or liberty except according to the procedure established by law, the procedure for arrest is not found in the Constitution itself but is specifically laid down in statutory law. Under the Code of Criminal Procedure, 1973 (CrPC), and now under its replacement, the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)⁴, detailed provisions exist regarding how an arrest must be made, the grounds of arrest, and the circumstances in which a person may be arrested with or without a warrant.⁵ Ultimately, in its traditional form, arrest means that the State authority takes the person into custody, assumes control over his body, and correspondingly imposes restrictions on his freedom of movement.

Meaning and Analysis digital restrictions

Nowadays, every person has to deal with two different worlds—one is the physical or manual world, and the other is the digital world, which we often call cyberspace. Accordingly, crimes and illegal activities can also spread in two ways: first, through physical movement and direct personal attacks; and second, without any bodily presence, by using digital tools and the internet. Example cyber-attack, phishing, virus, communal violence through online portal, hate speeches etc. In many cases, to curb online crimes that which is happening through websites, social media, or communication apps like WhatsApp, it may not always be necessary to arrest or detain the physical body of the offender. Instead, it becomes important to restrict their websites, accounts, and internet access so that their digital movement can be controlled. This way, the state essentially takes custody of the person's digital liberty and prevents them from spreading illegal content or committing crimes through any digital device or platform.

nuisance, or danger to public peace, Section 151: Preventive arrest to stop a cognizable offence, IT Act and Disaster Management Act 2005.

³ Article 21 of the Indian Constitution "No person shall be deprived of his life or personal liberty except according to procedure established by law."

⁴ Sections 35–60 BNSS, 2023.

⁵ Sections 41–60A Arrest under CrPC 1973.

The way arrest has not been defined anywhere only its process has been defined in that same way this two terms Digital arrest and digital restrictions is also does not have any statutory definition, however, as per the practices which is going on, the way digital restrictions has been done, digital restrictions can be defined as, where authorities control online data and communications platforms of suspect on the permitted ground to prevent illegal activities like hacking or cybercrimes or restricting or denying access to his electronic devices, digital platforms, websites, networks so that he should not commit any further crime etc. Many times, suspect has been kept in the surveillance of digital tools like camera, or ask to report through the digital cameras to the authority or kept under the surveillance of camera in his home itself.

Overall, digital restrictions therefore refer to process of digitally detaining an individual suspected of committing a crime in cyberspace. While it may sometimes involve physical detention, it more often focuses on restricting access to electronic devices, digital platforms, and networks, with the purpose of preventing further online crimes, securing electronic evidence, and protecting society from harm.⁶ Overall, we can say that digital restrictions technology is involved into any form to prevent crime, curb crime, etc.

It is necessary, however, to distinguish these lawful digital restrictions from the phenomenon popularly described as “digital arrest”, which is not a legal procedure at all but a form of cyber fraud. In such frauds, callers impersonating police, CBI or other officials accuse the victim of a crime, keep the victim on a video call for hours or even days, and use forged warrants, uniforms and staged online court hearings to extort money.⁷ In October 2024, the Prime Minister and the Union Home Minister publicly clarified that no government agency conducts investigations through phone or video calls.⁸

The scale of this fraud grew sharply before showing signs of decline. Data compiled by the Indian Cyber Crime Coordination Centre show that reported digital arrest cases rose from 39,925 in 2022, involving losses of about Rs 91 crore, to 1,23,672 in 2024, involving losses of about Rs 1,918 crore, before falling to 17,264 cases and Rs 644 crore in 2025 after sustained

⁶ What is Digital arrest and digital restrictions? What are Digital arrest and digital restrictions? - GeeksforGeeks, (visited on 26 August 2025)

⁷ Abhik Deb, “‘Felt like I Was under Hypnosis’: How Digital Arrest Scams Dupe Indians of Their Hard-Earned Money” *Scroll.in* (29 October 2024) <<https://scroll.in/article/1075007/feels-like-i-was-under-hypnosis-how-digital-arrest-scams-dupe-indians-of-their-hard-earned-money>> accessed 23 September 2026.

⁸ ‘Home Minister Shah Reaffirms Govt’s Commitment to Cyber Secure Bharat’ *All India Radio News* (New Delhi, 27 October 2024) <<https://www.newsonair.gov.in/home-minister-shah-reaffirms-govts-commitment-to-cyber-secure-bharat>> accessed 23 September 2026.

public awareness campaigns.⁹ The Union Government has also informed Parliament that more than 83,668 WhatsApp accounts linked to such frauds had been blocked, which shows that the State now relies on genuine digital restrictions to counter the false ones.¹⁰

Existing Law & Legislature to execute digital restrictions by authority

“What are the laws that empower the State machinery to carry out a *digital restriction*—that is, restricting an individual’s fundamental rights, liberty, and use of the internet¹¹—without physically arresting the person?” it’s an important question which need to analyse since the any fundamental rights, liberty can’t be curtailed without the due process of law. Hence, though digital restrictions person has not been manually arrested or kept in custody but still his access over the cyber space and in real world is monitored through the digital processes that’s the reason somewhere its need to study the laws on it.

Criminal Procedure Code/BNSS 2023

Section 144¹² of the CrPC/ 163 of BNSS¹³ empowers Magistrates to issue urgent prohibitory orders to prevent danger, disturbance, or breach of peace. Traditionally, it has been used to restrict assemblies, processions, and carrying of arms in physical spaces. In the digital age, however, this provision has been extended to control online activities and mass mobilization on social media. Authorities have in the past invoked it to impose internet shutdowns or block digital communication platforms, which effectively results in a form of “Digital arrest and digital restrictions” where liberty is curtailed without physical detention. The practice remains widespread, as Access Now and the #KeepItOn coalition recorded 65 internet shutdowns in India in 2025, keeping India among the leading countries in the world, out of at least 313 shutdowns documented across 52 countries that year.¹⁴ These orders can be passed *ex parte* and may apply to entire districts or states, with a maximum duration of two months, extendable up to six months by the State Government.

⁹ Ananya Bhardwaj, ‘After 465% Spike in 2024, MHA Data Shows Digital Arrest Scams Are on a Decline in India’ *ThePrint* (New Delhi, 18 February 2026) <<https://theprint.in/india/governance/after-465-spike-in-2024-mha-data-shows-digital-arrest-scams-are-on-a-decline-in-india/2857002/>> accessed 23 September 2026.

¹⁰ ‘Indians Lost INR 1,935 Cr to Digital Arrest Scams in 2024: Govt’ *Inc42* (14 March 2025) <<https://inc42.com/buzz/indians-lost-inr-1935-cr-to-digital-arrest-scams-in-2024-govt/>> accessed 23 September 2026.

¹¹ *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637

¹² Section 144 of CrPC 1973.

¹³ 163 of BNSS 2023.

¹⁴ ‘India Records 65 Internet Shutdowns in 2025, among Top Globally: Report’ *Business Standard* (New Delhi, 31 March 2026) <https://www.business-standard.com/amp/india-news/india-records-65-internet-shutdowns-2025-access-now-report-126033100877_1.html> accessed 23 September 2026; Access Now, ‘Rising and Resisting in the Darkness: Internet Shutdowns in 2025’ (31 March 2026) <<https://www.accessnow.org/press-release/rising-and-resisting-in-the-darkness-internet-shutdowns-in-2025/>> accessed 23 September 2026.

The same provision has more recently been used to restrict particular digital tools rather than the internet as a whole. District Magistrates in several districts of Jammu and Kashmir, first in Doda and Kishtwar and later in others including Srinagar, Budgam and Shopian, issued prohibitory orders banning the use of Virtual Private Networks on the ground that they could be used to evade monitoring and to spread inflammatory content.¹⁵ In Budgam alone, the police registered two FIRs and bound down eleven persons for using VPNs in breach of such an order, which shows how a general preventive power is now being used to regulate an individual's conduct in cyberspace.¹⁶

Information Technology Act 2000

A information technology Act 2000 is the one which dealing exclusively with those crimes which happening with the help of IT or through IT. In this Act state and Central have given power to asses or any agency to do asses intercept, monitor, or decrypt information through any computer resource on the ground of sovereignty, integrity, defence, security of the State, public order, or preventing incitement to offences.¹⁷ This power allows the State to monitor and intercept a person's digital communication, but it does not authorise house arrest or any other form of physical confinement. Other than that, state also have power to block websites, apps, or online platforms (e.g., TikTok, Chinese apps, pornographic content, hate speech portals). This provision is somewhere very close and connecting with the concept of Digital arrest and digital restrictions where state will get power to restrict persons online liberty accordingly.¹⁸ other than that, Social Media Companies, internet intermediaries must comply with government takedown orders. If due to some reasons if they fail to do so, then they lose "safe harbour" protection and become liable for user content. This indirectly enforces "Digital arrest and digital restrictions" of individuals by removing their online presence.¹⁹ Official figures reported in December 2024 show that 28,079 URLs were blocked under the Act's blocking power between 2022 and 2024, with Facebook and X together accounting for more than 21,000 of them.²⁰ Platforms also comply with the great majority of such demands, as X has disclosed that it received 29,118 removal requests from the Indian Government between

¹⁵ Jehangir Ali, 'Jammu and Kashmir Police Crack Down on VPN Use, File FIRs and Bind Down Dozens Across Districts' *The Wire* (Srinagar, 3 January 2026) <<https://thewire.in/rights/jammu-and-kashmir-police-crack-down-on-vpn-use-file-firs-and-bind-down-dozens-across-districts>> accessed 23 September 2026.

¹⁶ Ibid.

¹⁷ Section 69 of IT Act 2000.

¹⁸ Section 69A – Power to Block Public Access to Information

¹⁹ Section 79 & 79(3)(b) of IT Act 2000.

²⁰ 'Govt Blocks Record 28,000 URLs in 2024; Facebook, X Face Maximum Takedowns' *Business Standard* (New Delhi, 3 December 2024) <https://www.business-standard.com/technology/tech-news/govt-blocks-record-28-000-urls-in-2024-facebook-x-face-maximum-takedowns-124120300714_1.html> accessed 23 September 2026.

January and June 2025 and complied with 26,641 of them, a compliance rate of about 91.5 per cent.²¹ Other than that, this Act is also giving power to the state to treat certain online acts as terrorism and allows very strict action against those misusing the internet including punishment which may extend to imprisonment for life.²²

Telecommunication Act 2023

The Telecommunications Act, 2023 empowers the Central Government or a State Government, on the occurrence of a public emergency or in the interest of public safety, to direct that messages be intercepted or not transmitted and to order the suspension of any telecommunication service, including the internet. Under the Telecommunications (Temporary Suspension of Services) Rules, 2024, a suspension order must be published with reasons, cannot remain in force for more than fifteen days, and must be examined by a review committee. These powers are the closest parallel in this statute to digital restrictions, since they allow the State to cut off or monitor digital communication without any physical detention.²³

Grounds of digital restrictions

Generally, restrictions are imposed on an individual to prevent the commission of a crime that is anticipated but has not yet been committed. For such preventive measures, the grounds must be strong and legally justified. In the same way, when a person is digitally restricted by the authorities—such as by limiting their internet access or restricting the use of certain applications—there must also be strong grounds for doing so, since this involves curtailing their fundamental right to freely navigate the digital or cyber space. The recognized grounds for imposing such restrictions include the prevention of further crime²⁴, safeguarding the security and integrity of the State²⁵, maintenance of essential services²⁶, prevention of cognizable offences, and control of unlawful assemblies or activities.²⁷

Use of Digital Restrictions by the Judiciary and other authorities and its Validity

Shreya Singhal v. Union of India (2015) 5 SCC 1: The use of digital restrictions by the judiciary and other authorities must always be balanced against the fundamental rights guaranteed under

²¹ 'X Users Say Posts Blocked in India Under Section 69A Orders' *MediaNama* (11 March 2026) <<https://www.medianama.com/2026/03/223-x-users-report-posts-withheld-india-section-69a-no-reasons-given/>> accessed 23 September 2026.

²² Section 66 F of IT Act 2000.

²³ Telecommunications Act 2023, s 20; Telecommunications (Temporary Suspension of Services) Rules 2024; 'Government Notifies Telecommunications (Temporary Suspension of Services) Rules' (SCC Online Blog, 25 November 2024) <<https://www.scconline.com/blog/post/2024/11/25/government-notifies-telecommunications-temporary-suspension-of-services-rules>> accessed 23 September 2026.

²⁴ 151 of CRPC, 107-110 of CRPC, (BNSS)

²⁵ Article 19 (2), National Security Act 1980, Unlawful Activities (Prevention) Act 1967.

²⁶ Essential Services Maintenance Act (ESMA), 1968, Disaster Management Act, 2005 – Section 6 & 10.

²⁷ Section 41, 199 of CRPC, 129 and 144 of CRPC. (BNSS)

the Constitution, particularly the freedom of speech and expression under Article 19(1)(a). In *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A of the Information Technology Act, 2000, on the ground that it was vague, overbroad, and imposed disproportionate restrictions on online speech. The Court clarified that while the State has the power to impose restrictions in the digital space, such restrictions must fall strictly within the “reasonable restrictions” enumerated under Article 19(2), such as sovereignty and integrity of India, public order, decency, or incitement to an offence. The judgment became a landmark in defining the scope of digital restrictions, establishing that judicial and executive authorities cannot impose arbitrary or excessive controls over online activities merely on the basis of inconvenience or dissenting opinions. Instead, restrictions must be precise, narrowly tailored, and legally justified. Thus, the *Shreya Singhal* case highlights that digital restrictions, though necessary for preventing cybercrime and maintaining order, must always respect constitutional safeguards and cannot be misused as a tool for unwarranted censorship or suppression of digital freedom.²⁸

Anuradha Bhasin v. Union of India (2020), the Supreme Court dealt with the constitutional validity of internet shutdowns imposed in Jammu and Kashmir following the abrogation of Article 370. The petitioner, a journalist, challenged the restrictions as violative of the freedom of speech and expression under Article 19(1)(a) and the freedom to carry on trade and profession under Article 19(1)(g). The Court held that the right to freedom of speech and expression and the right to carry on business using the internet are constitutionally protected rights, subject only to reasonable restrictions under Article 19(2) and 19(6). Importantly, the Court directed that suspension of internet services must be temporary, proportionate, and subject to judicial review, and that indefinite internet shutdowns are impermissible. This judgment became a landmark in shaping the concept of digital restrictions in India, recognising both the necessity of digital curbs for security and public order, and the obligation to ensure that such restrictions do not disproportionately infringe upon fundamental rights.²⁹

Use of Digitalisation after the Arrest of Person

Gautam Navlakha v. National Investigation Agency (2021), the Supreme Court held that house arrest, when imposed with appropriate safeguards, could be treated as a valid form of custody for the purposes of investigation under the Unlawful Activities (Prevention) Act, 1967. However, on the facts of Navlakha’s own case, the Court held that his 34 days of house arrest

²⁸ *Shreya Singhal v. Union of India* (2015)

²⁹ *Anuradha Bhasin v. Union of India* (2020)

in 2018 could not be counted towards the 90-day period available to the investigating agency for filing a chargesheet, because that house arrest had not been ordered as custody under Section 167 of the Code of Criminal Procedure, and it dismissed his plea for default bail.³⁰ The technology-based restrictions came later, in November 2022, when the Supreme Court allowed him to be moved from prison to house arrest in Navi Mumbai on conditions that included CCTV cameras at the entry and exit points of the house and a bar on using the internet, a computer or any other communication device.³¹ By doing so, the judiciary recognized house arrest with digital restrictions as an effective and legally permissible alternative form of detention, balancing investigative needs with humanitarian concerns. This marked a progressive step in adapting traditional notions of custody to contemporary realities where technology can be deployed to monitor and restrict an accused without resorting solely to prison confinement.³²

Use of Digitalisation and Digital restrictions for imposing Bail Conditions

In *Devangana Kalita v. State of Delhi* (2021), arising from the Delhi riots conspiracy case, the Delhi High Court granted bail to the accused, a student activist charged under serious provisions including the Unlawful Activities (Prevention) Act (UAPA). While granting bail, the Court imposed strict conditions to ensure that her liberty did not interfere with the ongoing investigation. As reported, these conditions required her to surrender her passport, not to leave the country without permission, not to contact prosecution witnesses, and not to tamper with evidence or do anything that would prejudice the trial.³³ The reported conditions did not include a specific restriction on her use of social media, and the case is therefore better understood as an illustration of the general conditions that courts attach to bail, which are capable of being extended to an accused person's online conduct where the facts justify it.³⁴

Types digital restrictions after analyse

Arresting the Person into Custody and Restraining Him from Using Digital Platforms

³⁰ 'Here's Why Gautam Navlakha Was Not Able to Make a Case for Default Bail before the Supreme Court' (SCC Online Blog, 16 May 2021) <<https://www.sconline.com/blog/post/2021/05/16/heres-why-gautam-navlakha-was-not-able-to-make-a-case-for-default-bail-before-the-supreme-court/>> accessed 23 September 2026.

³¹ 'Supreme Court Allows Gautam Navlakha to Be Moved to House Arrest' *The Wire* (New Delhi, 10 November 2022) <<https://thewire.in/law/supreme-court-allows-gautam-navlakha-to-be-moved-to-house-arrest>> accessed 23 September 2026.

³² *Gautam Navlakha v. National Investigation Agency* (2021)

³³ Ritika Jain, 'Delhi HC Grants Bail to Devangana Kalita, Natasha Narwal, Asif Iqbal Tanha' *BOOM* (15 June 2021) <<https://www.boomlive.in/amp/law/delhi-high-court-delhi-riots-pinjara-tod-13529>> accessed 23 September 2026; 'Delhi HC Grants Bail to Devangana Kalita, Natasha Narwal, Asif Iqbal Tanha in UAPA Case' *ANI* (New Delhi, 15 June 2021) <<https://sg.news.yahoo.com/delhi-hc-grants-bail-devangana-055532942.html>> accessed 23 September 2026.

³⁴ *Devangana Kalita v. State of Delhi* (2021),

In certain cases, when an individual is arrested and taken into custody, authorities may simultaneously impose restrictions on the use of digital platforms, websites, or applications. This ensures that the accused cannot interfere with ongoing investigations, tamper with digital evidence, or incite further offences through online channels. Such measures are particularly relevant in cybercrime cases or situations where social media could be used to mobilize unrest. By combining physical custody with digital restrictions, law enforcement balances the need for security with the procedural safeguards of arrest.

Not Arresting the Person into Custody but Keeping Him under Digital Surveillance at Home

Sometimes, an individual may not be physically arrested, but law enforcement places them under digital surveillance at their residence. This can include monitoring their communication devices, tracking online activities, or using GPS and CCTV for location verification. Such surveillance allows authorities to prevent potential crimes while respecting the person's limited liberty, particularly in cases where physical detention is deemed unnecessary or disproportionate.

Such technology has already entered Indian practice. In November 2023, the Jammu and Kashmir Police became the first police force in the country to fit a GPS tracker anklet on an accused released on bail in a terror financing case, following an order of a Special Court in Jammu.³⁵ Researchers at Project 39A have cautioned, however, that such devices depend on satellite signals, mobile network coverage and battery life, are prone to false alarms, and may expose accused persons to allegations of breaching bail conditions for failures that are not their fault.³⁶

Not Arresting the Person Physically but Restricting Websites or Digital Use

A less intrusive method is where the accused is not taken into physical custody but is restricted from accessing certain websites, applications, or online services. This form of digital restriction prevents the individual from engaging in cyber offences or communicating with potential accomplices, while still allowing them to maintain daily life. Courts may impose such restrictions as part of bail conditions or preventive measures under cybercrime laws.

Daily Online Reporting

³⁵ Sakshi Jain, 'GPS Ankle Monitors for UAPA-Accused on Bail: Too Many Issues to Ignore' (Project 39A, National Law University Delhi, November 2023) <<https://www.project39a.com/writings/gps-ankle-monitors-for-uapa-accused-on-bail-too-many-issues-to-ignore>> accessed 23 September 2026.

³⁶ Ibid.

In some preventive or conditional liberty cases, authorities require the accused to report online daily to the investigating agency or probation officer. This digital reporting system ensures that the person remains accountable without the need for continuous physical monitoring. It allows authorities to track movements, verify compliance with bail conditions, and prevent potential offences, while the accused remains free to conduct their normal activities.

House Arrest with Digital Surveillance

House arrest combined with digital surveillance is a more intensive restriction where the individual is confined to their residence and monitored through technological means, such as CCTV cameras, GPS tracking, or restricted communication devices. This method serves as an alternative to conventional imprisonment, providing a controlled environment for investigation while minimizing human resource use by the authorities. It balances the investigatory or security needs of the state with humanitarian considerations and the rights of the accused

Challenges and Issues in Digital Restrictions

Legal Issues and ambiguity: One of the foremost challenges in implementing digital restrictions is the lack of a clear statutory definition. Terms such as “digital arrest” and “digital restrictions” do not exist in any codified law, leaving their interpretation largely to the courts and administrative authorities. As a result, authorities often rely on existing legislation such as the Information Technology Act, 2000, CrPC, and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) to justify digital measures. This ambiguity can lead to inconsistent application, varying standards across jurisdictions, and potential conflicts between executive orders and judicial scrutiny.

Fundamental Rights Concerns: Digital restrictions inherently involve curtailing access to cyberspace, which may affect constitutionally guaranteed rights. Restricting an individual’s online activity or access to digital platforms may violate Article 19(1)(a) (freedom of speech and expression), Article 21 (right to life and personal liberty), and the right to informational privacy as recognized in the landmark *Justice K.S. Puttaswamy v. Union of India (2017)* judgment. Without proper legal safeguards, such measures risk disproportionate interference with individual liberties, potentially undermining the balance between state security and personal freedoms.

Misuse and Overreach: There exists a significant risk of abuse in the application of digital restrictions. Authorities may impose arbitrary or excessive limitations under the pretext of preventing cybercrime or maintaining public order. In politically sensitive cases, there is

potential for misuse against activists, journalists, opposition leaders, or social media users, raising concerns of selective targeting and suppression of dissent. These concerns are not merely theoretical. In July 2021, the Pegasus Project, an international media investigation in which The Wire took part, reported that around 300 verified Indian mobile numbers, including those of ministers, opposition leaders, more than 40 journalists and several activists, appeared on a leaked list of potential targets of the Pegasus spyware, which its maker says it sells only to government agencies.³⁷ Forensic tests on a small sample of phones found signs of targeting in 37 devices, 10 of which were Indian.³⁸ Lack of oversight or accountability mechanisms further exacerbates the possibility of overreach.

Technological Limitations: Even when implemented with legal justification, digital restrictions face technological challenges. Digital surveillance tools, including facial recognition, GPS tracking, or monitoring apps, are not infallible and can be vulnerable to hacking, data breaches, or manipulation. False positives in identification systems, erroneous blocking of legitimate content, and technical glitches may unjustly affect individuals' rights. Replies obtained by the Internet Freedom Foundation under the Right to Information Act revealed that the Delhi Police treats a facial recognition match of 80 per cent similarity as a positive result, while lower scores are not discarded but treated as "false positives" that may still be investigated further.³⁹ The same replies disclosed that no privacy impact assessment of the technology had been carried out, even though it had been used to identify suspects in riot investigations.⁴⁰ Moreover, the rapid evolution of technology often outpaces regulatory and judicial mechanisms, creating gaps in protection and enforcement.

Enforcement and Compliance Issues: Digital restrictions require compliance from intermediaries such as social media platforms, internet service providers, and app developers. Delays, non-compliance, or inconsistent enforcement by these private entities can undermine the effectiveness of restrictions. Additionally, enforcing digital restrictions across jurisdictions, especially in cases of cross-border cybercrime, presents logistical and legal complexities. The difficulty is acute in digital arrest frauds, many of which are traced to organised scam centres in Thailand, Cambodia and Myanmar, so that the arrest of local agents and mule account

³⁷ Shemin Joy, 'Over 40 Indian Journalists, Activists on List of Potential Pegasus Surveillance Targets' *Deccan Herald* (New Delhi, 18 July 2021) <<https://www.deccanherald.com/india/over-40-indian-journalists-activists-on-list-of-potential-pegasus-surveillance-targets-1010155.html>> accessed 23 September 2026.

³⁸ *Ibid.*

³⁹ Vallari Sanzgiri, 'Delhi Police's Reply to IFF RTI Shows FRT May Worsen Religious-Bias in Policing' *MediaNama* (18 August 2022) <<https://www.medianama.com/2022/08/223-delhi-police-iff-rti-facial-recognition-80-percent-accuracy/>> accessed 23 September 2026.

⁴⁰ *Ibid.*

holders in India barely affects the operators abroad.⁴¹ Recovery also remains limited, as officials report that only about 19 per cent of defrauded money is now blocked before it reaches the fraudsters, up from 6 per cent in 2021.⁴²

Psychological and Social Impact: Restricting digital access can have broader social and psychological effects. Individuals under digital restrictions may experience isolation, reduced access to information, and disruption of professional or educational activities. Victims of digital arrest frauds experience this harm in an extreme form, since they are ordered to remain on continuous video calls and not to contact anyone while impostors interrogate them, and experts note that elderly and retired persons, who often have limited digital literacy and are anxious about their reputation, are especially vulnerable.⁴³ Official data point in the same direction, with crimes against senior citizens rising by 16.9 per cent to 32,602 cases in 2024, a rise that officials link largely to online financial fraud.⁴⁴ Unlike physical detention, which is more visible and regulated, digital confinement often occurs in private spaces, making oversight and accountability more challenging.

Conclusion

Digitalization has transformed the landscape of crime and law enforcement, introducing both new opportunities and challenges for the criminal justice system. While traditional arrests and preventive measures continue to play a crucial role in maintaining public order, digital restrictions have emerged as an important tool to prevent, monitor, and control cybercrime. Through measures such as restricting access to websites, monitoring online activities, house arrest with digital surveillance, and imposing bail conditions with online limitations, authorities can effectively curb criminal activity in cyberspace without always resorting to physical detention.

However, the absence of a clear statutory definition for concepts like “digital arrest” or “digital restrictions” creates legal ambiguity. There are significant concerns about the potential infringement of fundamental rights, misuse by authorities, technological limitations, and enforcement challenges. Landmark judicial interventions, such as *Shreya Singhal v. Union of India* and *Anuradha Bhasin v. Union of India*, have underscored the need for proportionality, legality, and respect for constitutional freedoms in the application of digital restrictions. Cases like *Gautam Navlakha* and *Devangana Kalita* demonstrate that courts are willing to integrate

⁴¹ Bhardwaj (n 9).

⁴² Ibid.

⁴³ Deb (n 7).

⁴⁴ Debroy (n 1).

digital surveillance and restrictions into custodial and bail conditions, provided there is a strong legal basis and adequate safeguards.

Overall, digital restrictions represent a necessary evolution of preventive law enforcement, but their application must carefully balance state security, public order, and individual rights. Without proper legal recognition and safeguards, there is a risk of arbitrary or disproportionate curtailment of liberty in cyberspace.

Suggestions

- **Statutory Clarity** – Introduce clear definitions of “digital arrest” and “digital restrictions” within the legal framework to remove ambiguity and ensure uniform application.
- **Judicial Oversight** – All digital restrictions should be subject to judicial review to ensure legality, necessity, and proportionality.
- **Proportional and Targeted Measures** – Digital restrictions should be narrowly tailored to prevent specific crimes, avoiding broad or indefinite curbs on online liberty.
- **Duration and Transparency** – Digital restrictions must have clearly defined time limits, with authorities maintaining records of imposed restrictions.
- **Safeguards for Fundamental Rights** – Ensure compliance with Articles 19 and 21, and the right to privacy, with mechanisms to challenge restrictions if misapplied.
- **Technological Accuracy and Security** – Use reliable, secure, and audited digital tools to prevent errors, hacking, or misuse in monitoring or restriction.
- **Accountability of Intermediaries** – Platforms and service providers must be clearly guided and legally obligated to comply with restrictions while respecting privacy and free speech.
- **Training and Awareness** – Law enforcement and judiciary should receive training in cybercrime, digital surveillance, and ethical use of digital restriction tools.