Page: 1200-1235 *URL: www.lijdlr.com*

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 4

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.171

CYBERCRIME POLICING VS. CITIZEN RIGHTS: A STUDY ON BANK ACCOUNT FREEZING IN INDIA

Rishabh Bahadur Singh[1]

I. ABSTRACT

Cybercrime has rapidly emerged as one of India's most complex law enforcement challenges, fuelled by the explosive growth of digital payments and the increasing sophistication of online fraud. To prevent dissipation of suspected proceeds of crime, Cyber Cells frequently resort to freezing bank accounts under Section 102 of the Code of Criminal Procedure. However, my study reveals that such freezes are often imposed without adequate scrutiny, notice, or judicial oversight, resulting in significant procedural and constitutional concerns. This research analyzes how these practices intersect with fundamental rights under Articles 14, 19(1)(g), 21, and 300A, and highlights the profound financial, emotional, and professional hardships experienced by innocent citizens caught in the investigative net. Through doctrinal analysis, case law review, and comparative assessment with safeguards in the UK, US, and EU, the study demonstrates that the current Indian framework lacks standardized procedures, transparency, and accessible redressal mechanisms. The findings emphasize the urgent need for reform, ranging from mandatory notice requirements and periodic review of freezing orders to clear SOPs for Cyber Cells and strengthened grievance pathways. Ultimately, the study argues that effective cybercrime control and protection of civil liberties are not competing objectives but essential complements. A balanced, rights-respecting approach is indispensable to ensure that digital policing enhances public trust rather than undermining it.

II. KEYWORDS

Cybercrime, Bank Account Freezing, Constitutional Safeguards, Due Process, Cyber Cells, Financial Vulnerability

[1] Lawyer Based in (India). Email: rishabhchintels@gmail.com

III. INTRODUCTION

A. BACKGROUND OF CYBERCRIME GROWTH IN INDIA

India's rapid digital transformation has brought millions into the fold of online banking, e-commerce, and real-time payments. In my opinion, while this shift has fuelled economic inclusion, it has also created an environment where cybercrime grows in both complexity and scale. Cyber fraud complaints—ranging from UPI scams to identity theft and fraudulent digital lending—have surged dramatically in the past decade. The very technologies that empower citizens have simultaneously made them vulnerable to sophisticated cybercriminal networks that exploit digital loopholes, social engineering, and fragmented law-enforcement mechanisms.

The law enforcement response to this surge has been to expand the mandate and powers of Cyber Cells across states. These agencies often operate under intense pressure to curb digital fraud swiftly, recover stolen funds, and prevent further losses. One of the tools increasingly deployed is the freezing of bank accounts suspected of receiving or routing fraudulent deposits. While necessary in genuine cases, this power—when exercised mechanically or without procedural checks—can disrupt lives as much as it aims to protect them.

B. RISE OF DIGITAL PAYMENTS AND FINANCIAL VULNERABILITY

India's financial ecosystem has undergone unprecedented change with the introduction of UPI, mobile wallets, and instant banking. Digital transactions today outnumber traditional cash operations, signalling deep trust in technology-driven convenience. However, this trust has created fertile ground for exploitation. Instant payments mean instant losses; a momentary lapse can result in money moving across multiple accounts within seconds, leaving little time for recovery.

According to me, ordinary citizens, small workers, gig-economy participants, and micro-entrepreneurs—who rely on modest and periodic digital income—are often the most exposed. When such individuals find their accounts suddenly frozen on suspicion alone, the consequences can be severe: withheld salaries, inability to pay bills, disruption of daily life, and emotional distress. These vulnerabilities underscore

the urgent need for safeguards that protect both financial systems and the dignity of individuals.

C. IMPORTANCE OF BALANCING SECURITY AND FUNDAMENTAL RIGHTS

Cybercrime investigations undeniably serve an essential public function: safeguarding financial integrity and protecting victims. But in pursuing crime control, the State must not sidestep the Constitution's promise of fairness, dignity, and due process. Freezing a bank account—while effective as an immediate preventive measure—directly touches upon fundamental rights: the right to life and livelihood (Article 21), the right to practice any profession (Article 19(1)(g)), the right to equality (Article 14), and the right to property (Article 300A).

The challenge, therefore, is not merely operational or technical—it is constitutional. When enforcement actions are taken without notice, without recorded reasons, or without informing the Magistrate, the line between protection and overreach blurs. Innocent individuals become collateral damage in the pursuit of efficiency. The State's duty to maintain cybersecurity cannot be allowed to eclipse its duty to uphold civil liberties. Striking the right balance between public interest and individual rights is thus central to a democratic rule-of-law society.

D. PURPOSE AND SCOPE OF THE STUDY

In my study, I have tried to critically examine the legality, legitimacy, and constitutional validity of bank account freezing in cybercrime investigations in India. It explores how Cyber Cells use their powers under Section 102 of the CrPC, how these powers are applied in practice, and whether procedural safeguards meant to prevent abuse are being consistently followed. Through analysis of case law, statutory provisions, and lived experiences of affected individuals, the research aims to reveal gaps between law and practice.

The scope extends beyond doctrinal analysis; it includes the human dimension—how arbitrary or mechanical freezing affects livelihoods, creates financial trauma, and undermines confidence in the justice system. By connecting constitutional principles with everyday realities, the study aims to highlight the need for a more transparent,

accountable, and rights-respecting approach to cybercrime policing. Ultimately, the research aspires to propose reforms that preserve both security and justice, ensuring that innocent citizens are never the silent victims of the system meant to protect them.

E. RESEARCH QUESTIONS

- Are current freezing practices constitutionally compliant?
- What procedural safeguards are being bypassed?
- How do international jurisdictions balance security and rights?

F. HYPOTHESIS

"Bank account freezing by Cybercrime authorities in India is frequently conducted without adherence to mandatory procedural and constitutional safeguards, resulting in arbitrary deprivation of property and violation of citizen rights."

G. RESEARCH METHODOLOGY

The research methodology employed in this study is primarily doctrinal, involving a comprehensive analysis of legal frameworks, case law, and constitutional principles related to bank account freezing in cybercrime investigations. It includes a detailed review of statutory provisions, particularly Section 102 of the CrPC and the Information Technology Act, 2000, alongside comparative assessments of practices in jurisdictions like the UK, US, and EU. The study also incorporates a qualitative approach, analyzing real-life case studies and personal accounts from individuals impacted by account freezes, thus blending legal analysis with human impact evaluation. Through this approach, the research aims to identify procedural gaps and propose reforms for a more transparent, rights-respecting system.

IV. LEGAL FRAMEWORK GOVERNING BANK ACCOUNT FREEZING

A. SECTION 102 OF THE CODE OF CRIMINAL PROCEDURE (CRPC)

Section 102 CrPC forms the backbone of the police's power to seize "property" connected to an offence, and in modern practice, bank accounts have been interpreted as property. This provision, originally drafted in a pre-digital era, is now stretched to

accommodate cybercrime investigations. Under this section, a police officer may seize any property suspected of being linked to a crime. In cybercrime cases, this is often interpreted broadly: even a ₹4,000 deposit into an innocent gig worker's account can trigger suspicion if the sender is later accused of fraud. However, the law does not grant unfettered power. It imposes three crucial safeguards.

- The officer must have reasonable suspicion, not speculative doubt.
- Reasons for seizure must be recorded to prevent arbitrary action.
- The Magistrate must be informed "forthwith", ensuring judicial oversight.

In reality, this last requirement is frequently ignored. For example, an individual whose Paytm-linked bank account received a legitimate payment from a friend reported that his account was frozen for weeks without any FIR or Magistrate oversight. Such cases highlight how a preventive tool can morph into a punitive measure if procedural checks are neglected.

B. INFORMATION TECHNOLOGY ACT, 2000 – RELEVANT PROVISIONS

The Information Technology Act does not directly authorize bank account freezing. Instead, it defines various cyber offences—identity theft, cheating by personation, data theft—under which police initiate investigations.

Sections dealing with:

- Unauthorised access,
- Computer-related fraud,
- Dishonest online inducements often become the basis for tracking financial trails. Once an offence under this Act is suspected, police rely on Section 102 CrPC to freeze accounts involved in the digital money trail.

What complicates matters is that digital money trails are often imperfect. Payments can route through multiple innocent accounts—delivery partners, freelancers, students—who simply received legitimate payments from someone later identified as an accused. Thus, while the IT Act sets the stage for investigation, it is not a licence for

arbitrary deprivation. The intersection of the IT Act and CrPC must be navigated with care, precision, and strict adherence to due process.

C. RBI GUIDELINES ON TRANSACTION MONITORING & FREEZING

The Reserve Bank of India plays a regulatory role in safeguarding the financial ecosystem.

RBI requires banks to:

- Monitor suspicious transactions,
- Flag unusual account behaviour under the "STR" (Suspicious Transaction Report) mechanism,
- Cooperate with law enforcement when mandated.

However, RBI does not authorize the arbitrary freezing of accounts. The bank cannot freeze an account unless:

- They receive a formal written request from the police, or
- The freeze is mandated under special laws like PMLA, or
- Court/tribunal orders are issued.

Banks often freeze accounts immediately upon receiving a police letter, sometimes without verifying its legal sufficiency. For example, a bank in Mumbai froze a customer's account because the Cyber Cell asked for it verbally—without any written order. While the bank acted out of fear of non-compliance, the customer's savings became inaccessible overnight, pushing him into debt for daily expenses. RBI guidelines emphasize procedural propriety and documentation, yet in practice, compliance varies depending on the bank's internal caution and the pressure of law enforcement.

D. PMLA AND FINANCIAL SURVEILLANCE MECHANISMS

The Prevention of Money Laundering Act (PMLA) provides a more structured but stringent framework for freezing bank accounts.

It is invoked in cases involving:

- Laundering of cyber fraud proceeds,
- Large-scale financial scams,
- Organized digital crime networks,
- Suspicious cross-border transfers.

Under PMLA, the Enforcement Directorate (ED) has the power to freeze accounts, but only after:

- Recording "reasons to believe,"
- Issuing a formal order,
- Notifying the Adjudicating Authority, and
- Allowing the affected individual to file objections.

Unlike Section 102 CrPC, PMLA has inbuilt checks and appeal mechanisms. The problem arises when police or cyber cells use the logic of PMLA (protecting financial integrity) but the procedure of CrPC (quick freezing without notice), resulting in a hybrid system where rights become collateral damage. For example, a small textile vendor's account was frozen because it received ₹50,000 from a person accused of a digital lottery scam. ED later clarified it had no involvement. The freeze had come solely from the cyber police—yet the impact on the vendor resembled the severity of a PMLA action, without the accompanying safeguards.

V. CONSTITUTIONAL SAFEGUARDS AND CITIZEN RIGHTS

A. ARTICLE 14 – PROTECTION FROM ARBITRARY STATE ACTION

Article 14 stands as a constitutional shield against arbitrary, discriminatory, or irrational actions of the State. When a citizen's bank account is frozen without notice, without recorded reasons, or without judicial oversight, it represents more than a procedural lapse—it is a retreat from the promise of equal protection under law.

Arbitrariness is the antithesis of equality. If two citizens in identical circumstances receive different treatment—one gets notice before a freeze, another receives none—Article 14 is violated. Even in situations involving cybercrime, where the State must act swiftly, the Constitution does not allow efficiency to replace fairness.

The freezing of an account without informing the depositor or without demonstrating the necessity of the action creates a situation where the individual is left defenseless, unable to challenge or even understand the action taken. Article 14 demands a rational nexus between suspicion and action—an expectation often unmet in mechanical or bulk freezing orders.

B. ARTICLE 19(1)(G) – RIGHT TO PROFESSION & LIVELIHOOD

For millions of Indians who rely on digital payments—gig workers, freelancers, small merchants, service providers—access to their bank account is not a luxury; it is the foundation of their livelihood. Article 19(1)(g) guarantees the freedom to practice any profession or carry on any occupation. When a bank account is frozen without cause or clarity, this freedom is directly impeded.

Consider a delivery worker or a tuition teacher receiving small periodic digital payments. The sudden freezing of an account, even for amounts as low as ₹4,000, can bring their earning capacity to a standstill. They cannot receive payments, pay rent, or sustain daily needs. The restriction may not be framed as a "ban on profession," but in outcome, it often operates as one. Thus, while the State may regulate economic activity in the interest of the general public, such regulation must be reasonable, and reasonableness collapses when due process is ignored.

C. ARTICLE 21 – DUE PROCESS & RIGHT TO LIFE/LIVELIHOOD

Article 21, under the Constitution of India, guarantees that no person shall be deprived of life or personal liberty except according to a "just, fair, and reasonable" procedure. The Supreme Court has interpreted "life" to include dignity, and "livelihood" as an essential component of that dignity. Freezing a citizen's bank account without informing them, without giving them an opportunity to explain, and without judicial supervision effectively cuts off their financial lifeline. For many individuals, it is equivalent to depriving them of the ability to survive.

Due process is not a mere technical formality—it is the constitutional recognition that the State's actions must respect human dignity. When Cyber Cells freeze accounts

based on suspicion alone, without proportionality or procedural integrity, the action becomes constitutionally suspect under Article 21.

D. ARTICLE 300A – RIGHT TO PROPERTY

Article 300A asserts that no person shall be deprived of their property except by authority of law. Money held in a bank account is a legally recognized form of property. Any deprivation—such as an account freeze—must therefore follow a lawful, transparent, and justified process.

When an authority freezes an account without:

- a written order,
- recorded reasons,
- communication to the holder, or
- judicial approval,

The deprivation ceases to be "by authority of law" and becomes an unconstitutional act. This Article bridges the gap between financial control and personal security—reminding the State that property cannot be suspended merely because it is convenient to do so during an investigation.

E. PRINCIPLES OF NATURAL JUSTICE IN SEIZURE PROCEEDINGS

Behind every constitutional guarantee lies a foundational principle: audi alteram partem—the right to be heard. Natural justice requires that a person be deprived of property or livelihood.

- Informed of the action,
- Given reasons,
- Offered an opportunity to respond, and
- Allowed access to a fair and impartial adjudicator.

In practice, many individuals whose accounts are frozen learn of the action only when routine payments bounce or ATM withdrawals fail. They are often unaware of the case number, allegation, or even the police unit involved. This creates an environment

where innocence becomes irrelevant until proven—flipping the presumption of innocence on its head. Natural justice does not demand elaborate hearings in every cybercrime freeze. But it does demand minimum fairness: timely notice, clarity of reasons, and a chance to contest. When these are missing, the freeze becomes not just procedurally defective but morally untenable.

VI. PROCEDURAL REQUIREMENT FOR ACCOUNT FREEZING

A. MANDATORY CONDITIONS UNDER SECTION 102 CRPC

Section 102 of the Code of Criminal Procedure, 1973, empowers police to seize "property" suspected of being linked to an offence. Over time, the courts have clarified that this includes bank accounts. Yet, this power is not absolute; it hinges on the presence of reasonable suspicion. The suspicion must be grounded in identifiable circumstances—such as a complaint linking a particular transaction to a fraudulent activity—not mere intuition or broad association. A ₹4,000 deposit to an innocent worker cannot be equated with proceeds of crime simply because the sender happens to be an accused in another matter.

Thus, before freezing an account, the officer must satisfy three essential criteria:

- The property (bank account) must be connected to the offence.
- There must be reasonable grounds for such belief.
- The seizure must be necessary for investigation.

When these criteria are applied carelessly or mechanically, the result is not better policing—it is procedural overreach, often harming those who have no knowledge of the underlying complaint.

B. REQUIREMENT TO INFORM THE MAGISTRATE

Section 102(3) expressly mandates that once property is seized, the police officer must "forthwith" report the seizure to the jurisdictional Magistrate. This requirement is not a mere formality; it is the constitutional checkpoint that ensures accountability.

Judicial oversight acts as a safeguard against:

- impulsive or hurried seizures,

- investigative bias,
- lack of application of the mind.

Yet in practice, this step is frequently bypassed. Many individuals only learn of their account freezing when they attempt a transaction at an ATM. Meanwhile, no Magistrate has reviewed whether the freeze was justified. This absence of judicial scrutiny transforms a temporary preventive action into an indefinite punishment, contrary to the design of the procedural law.

C. DUTY TO NOTIFY THE ACCOUNT HOLDER

Natural justice demands that the person whose account is frozen must be informed promptly. However, many victims of wrongful freezes describe the same experience: silence. Banks decline to share documents. Cyber Cells remain unreachable. No copy of any order is provided, no reason communicated, and no direction on how to seek redress.

In law, the duty to notify flows from:

- constitutional guarantees of fairness,
- the right to challenge the action,
- the need to prevent disproportionate hardship.

A citizen cannot defend themselves against an invisible order. Notification is not a courtesy; it is a prerequisite for procedural fairness. Without it, the freeze becomes arbitrary—even if the police had genuine investigative concerns.

D. BURDEN OF RECORDING REASONS IN WRITING

Every seizure under Section 102 requires the officer to record reasons in writing. This protects both the investigation and the citizen.

Written reasons show:

- why the freeze was necessary,
- how the account was connected to the offence,
- whether alternatives were considered.

A simple example illustrates the importance: Suppose a cyber officer freezes ten accounts involved in a suspected fraud trail. If the officer fails to document the rationale for each freeze, innocent intermediaries—cab drivers, freelancers, homemakers—get trapped in the police net without justification. Written reasons force the officer to think, evaluate, and justify. Courts consistently hold that undocumented suspicions cannot pass the test of legality. A freeze without reasons is a freeze without a legal foundation.

E. TIME LIMITS, REVIEW PROCEDURES & PROPORTIONALITY

Indian law does not permit indefinite freezing. Even when an account must be frozen, the action must satisfy the principle of proportionality—the freeze must not be broader, longer, or harsher than necessary.

Key expectations include:

- Reasonable time limits: A freeze must be reviewed periodically; investigations cannot rely on prolonged financial deprivation.
- Proportionality of scope: The freeze should target only the amount under suspicion, not the entire account, unless necessary.
- Review by senior officers: Supervisory oversight prevents misuse by lower-level investigators.
- Opportunity to seek modification or partial unfreeze: For essential expenses, business continuity, or medical needs.

In practice, many individuals face open-ended freezes lasting months, sometimes years, even when no formal charge is filed or when investigations stagnate. Such indefinite restrictions transform a preventive tool into a punitive sanction—something no procedural law authorizes.

VII. PROCEDURAL IRREGULARITIES IN CYBER POLICING

A. FREEZING WITHOUT FIR OR FORMAL INQUIRY

One of the most troubling tendencies in cyber policing is the freezing of bank accounts even before the registration of a First Information Report (FIR). Although Section 102

CrPC allows seizure of property suspected to be linked to a crime, it does not envision such power being exercised in a legal vacuum.

Freezing an account without an FIR strips the citizen of any formal avenue to seek information or remedy. Without a case number or allegation on record, the individual is left in a state of limbo—unable to know who complained, what the suspicion is, or how to challenge the action.

For instance, a college student receiving a small digital transfer from a friend later implicated in a cyber fraud may suddenly find his account frozen, not because of evidence, but because the friend's name appears in an informal police note. Without an FIR, the freeze becomes an act of administrative convenience rather than a lawful procedure.

B. ABSENCE OF NOTICE TO THE ACCOUNT HOLDER

One of the most human dimensions of procedural irregularity is the silence that accompanies most freezing orders. Citizens often discover the freeze not through official communication but through failed ATM withdrawals, bounced UPI payments, or employer complaints about rejected salary transfers.

The lack of notice:

- deprives them of the chance to clarify legitimate transactions,
- prevents them from preparing documentation to prove innocence,
- creates immediate financial hardship, and
- psychologically frames them as "suspects" without explanation.

Take the case of a delivery worker who receives daily micro-payments via UPI. A sudden freeze—even over a disputed payment as small as ₹500—can disrupt his ability to pay for fuel, food, and rent. The absence of notice transforms an investigative precaution into a punishment without trial.

C. FAILURE TO INFORM MAGISTRATE (COMMON LAPSE)

Perhaps the most fundamental procedural irregularity is the repeated failure of police to inform the jurisdictional Magistrate after freezing a bank account, as mandated under Section 102(3) CrPC.

Judicial oversight ensures that:

- the freeze is based on reason, not assumption,
- the police do not exceed their mandate,
- The citizen has an institutional protector of rights.

In numerous real-world cases, this step is simply ignored. A cyber officer may freeze dozens of accounts in a single batch, often based on a forwarded complaint from another district or state. Without notifying the Magistrate, the freeze lacks the judicial legitimacy required by law. The result is an action that appears lawful on paper but is constitutionally defective—a serious irregularity that compromises both fairness and the integrity of the investigation.

D. MECHANICAL OR ALGORITHM-BASED FREEZING

As digital policing expands, some Cyber Cells rely on automated systems that flag "suspicious" accounts based on transaction patterns or link analysis. While such tools are useful for preliminary screening, problems arise when freezing orders are issued mechanically, without human oversight or contextual evaluation.

Examples include:

- Accounts frozen solely because they received money from another frozen account,
- Innocent intermediaries caught in "chain freezing" where suspicion cascades through multiple accounts,
- Freelancers or small shop owners are targeted because they receive varied digital payments.

Algorithms can detect patterns but cannot distinguish between fraud proceeds and everyday financial life. A florist receiving payments from hundreds of customers may

look like a "high-volume transaction node," but human review would instantly reveal the benign nature of the business. Unchecked automation can therefore magnify errors and freeze the wrong accounts.

E. EXCESSIVE AND DISPROPORTIONATE USE OF POWER

Proportionality—freezing only what is necessary—is a cornerstone of lawful seizure. Yet in practice, Cyber Cells frequently impose blanket freezes on entire accounts, even when the suspected amount is tiny. Imagine a domestic worker whose account holds ₹40,000 in savings but receives a disputed deposit of ₹1,200. Instead of freezing only the questionable amount, the entire balance becomes inaccessible.

This kind of disproportionate action causes:

- complete financial paralysis,
- inability to meet daily needs,
- long-lasting emotional distress,
- unintended stigmatization within families and communities.

Moreover, freezes often continue for months with no periodic review, turning what should be a temporary investigative tool into an indefinite deprivation of financial autonomy. Such misuse extends beyond procedural irregularity—it crosses into a violation of fundamental rights and undermines trust in digital policing.

VIII. JUDICIAL PRECEDENTS AND CASE LAW ANALYSIS

Judicial scrutiny plays a crucial role in restoring balance when investigative enthusiasm eclipses constitutional boundaries. Indian courts have repeatedly emphasized that the power to freeze bank accounts must be exercised with restraint, transparency, and strict compliance with procedure. Through their rulings, courts highlight that efficiency in cybercrime control cannot override fairness in governance.

A. TEESTA ATUL SETALVAD V. STATE OF GUJARAT (2018) 2 SCC 372

In this landmark case, the Supreme Court underscored that freezing a bank account is a serious intrusion into an individual's financial autonomy and therefore must be supported by recorded reasons and immediate judicial oversight.

The Court clarified that:

- Police cannot operate on vague suspicion.
- Reasons for freezing must be cogent and traceable.
- Magistrates must be informed without delay.

This judgment resonates deeply in cybercrime contexts where banks and Cyber Cells often freeze accounts in bulk without detailed justification. The ruling serves as a reminder that even in digital investigations, constitutional discipline cannot be abandoned.

B. SWARAN SABHARWAL V. COMMISSIONER OF POLICE 1988 CRI LJ 241 (DELHI HIGH COURT)

The Delhi High Court examined a scenario where the petitioner discovered the freeze only after routine transactions began failing. The Court held that non-communication of the freezing order amounts to a violation of natural justice and Article 21.

The Court observed:

- Citizens cannot be blindsided by silence.
- The right to be informed is integral to dignity.
- Without notice, a freeze becomes punitive rather than preventive.

This case illustrates a common real-world experience: people learning about freezes through ATM failures rather than official communication. Courts have repeatedly condemned such opaque practices as unconstitutional.

C. KISHORE KUMAR V. STATE OF KERALA

In this case, the Kerala High Court confronted a situation strikingly similar to what many innocent individuals experience today. The petitioner's account was frozen merely because funds had passed through it, with no evidence of involvement in the alleged fraud.

The Court held:

- Mere receipt of money does not create criminal liability.

- Police must establish a direct nexus between the alleged offence and the frozen account.
- Absent such nexus, the freeze is unlawful.

Importantly, the Court ordered the defreezing of the account, reinforcing that suspicion cannot substitute for proof or procedure.

D. PRAGYA SINGH THAKUR V. STATE OF MAHARASHTRA

Though not specifically about cybercrime, this Supreme Court decision emphasizes that State power must be exercised within constitutional limits, and procedural lapses cannot be justified in the name of investigation.

The Court stressed:

- Investigative convenience cannot override statutory safeguards.
- Judicial oversight is not optional; it is a constitutional necessity.

This reasoning is fully applicable to cyber policing, where the desire to immediately secure funds often results in cutting procedural corners.

E. PATTERNS EMERGING FROM JUDICIAL INTERPRETATION

Across diverse cases, courts consistently articulate the same principles.

- **Procedural compliance is non-negotiable:** Failure to notify the Magistrate or the account holder renders the freeze vulnerable to judicial challenge.
- **No inference of guilt from mere transaction trails:** Money moving through an account is insufficient to treat the holder as complicit.
- **Proportionality governs all freezing actions:** Courts disapprove indiscriminate freezing of entire accounts when only a fraction of the funds is disputed.
- **Human impact matters:** Courts increasingly acknowledge the severe livelihood disruption caused by arbitrary freezes, especially for wage earners, freelancers, and small business owners.

- **Judicial oversight restores balance:** High Courts often become the primary forum for relief, highlighting gaps in administrative accountability.
- **Judicial Approach: A Human Lens on Digital Investigations:** Indian courts have adopted a distinctly human-centred perspective, recognizing that the digital economy is deeply intertwined with everyday survival. When police freeze accounts mechanically, the courts treat such action not merely as a legal misstep but as a human rights concern.
- **Judges have repeatedly acknowledged:**
    - The emotional stress caused by losing access to savings,
    - The humiliation of being labelled a suspect without explanation,
    - The economic instability inflicted on families and dependents.

Judicial discourse thus bridges law and lived experience, ensuring constitutional compassion in a technologically evolving legal landscape.

IX. IMPACT ON CITIZENS

A. FINANCIAL HARDSHIP AND LIVELIHOOD LOSS

For many Indians, especially those in the gig economy or informal sector, a bank account is not merely a financial tool—it is the core of their livelihood. When an account is suddenly frozen, even temporarily, the consequences can be immediate and devastating. Income halts without warning. Daily expenses—food, fuel, rent, school fees—become impossible to manage.

A delivery worker who receives dozens of small UPI credits each day may find himself unable to top up fuel to continue working. A home-based tailor who depends on online payments may suddenly be unable to receive customer advances. A student who relies on digital transfers from family may find herself stranded without funds to pay for transportation or meals. Even when the disputed amount is tiny—₹500, ₹1,200, or ₹4,000—the entire balance is often frozen, placing the citizen in a financial chokehold. A preventive measure meant for protecting victims inadvertently

transforms into a punishment imposed on someone who may never have been accused of wrongdoing.

B. SOCIAL, EMOTIONAL, AND PROFESSIONAL CONSEQUENCES

The impact of an account freeze extends far beyond finances. It carries a social and psychological weight that law enforcement rarely acknowledges. Families begin to doubt the individual's honesty when the bank refuses to explain the freeze. Employers become suspicious or impatient, assuming misconduct. Friends and relatives may distance themselves due to perceived criminal involvement. Emotionally, the uncertainty is draining. Citizens often describe feeling powerless, humiliated, or criminalized despite having done nothing wrong.

They face:

- Stress and anxiety from not knowing the allegation,
- Shame when payments bounce, or employers question them,
- Fear of long-term consequences on their reputation.

Professionally, the inability to transact affects credibility. Freelancers may lose clients. Merchants may lose customers. Even salaried employees face embarrassment when salaries fail to be credited. These are not collateral effects—they are human costs borne in silence by those caught in procedural crossfire.

C. LIMITED AVENUES OF ADMINISTRATIVE REDRESS

One of the most painful realities for affected citizens is the near absence of accessible administrative remedies. Banks often respond mechanically—"We cannot unfreeze without police instructions"—leaving the individual trapped between two institutions, neither of which takes responsibility for transparency. Cyber Cells may be understaffed, overburdened, or simply unwilling to engage.

Many citizens report:

- Phone numbers that go unanswered,
- Officials asking them to "wait indefinitely,"
- No copy of the freezing order is being provided.

- No explanation of the next steps or required documents.

Without an FIR number or a written order, the citizen cannot even file a formal complaint. The system thus creates an information vacuum, where the person whose rights are directly affected struggles to find a door to knock on. The lack of structured administrative channels forces ordinary people—who may not understand legal procedures—to navigate complex bureaucratic or judicial processes simply to regain access to their own money.

D. DELAY IN UNFREEZING & JUDICIAL BURDEN

The absence of timely administrative review pushes most affected citizens toward the judiciary, particularly the High Courts. But judicial pathways are time-consuming, expensive, and emotionally taxing. For someone whose savings are locked, waiting two months for a hearing is not a minor inconvenience—it is a matter of survival. Many cannot afford legal counsel. Others cannot afford the time. And even when courts finally order the freeze to be lifted, the delay often nullifies the relief: rent deadlines are missed, businesses collapse, trust erodes.

This cycle has a broader institutional impact as well. Courts are forced to intervene repeatedly in matters that should have been resolved administratively with clear protocols. Judges become the de facto oversight mechanism because police and banks lack internal review systems. In the long run, this burdens the judiciary and undermines public confidence in both digital governance and cyber policing.

E. ANALYTICAL SYNTHESIS: A HUMAN CRISIS HIDDEN IN TECHNICAL PROCEDURE

The freezing of bank accounts is often treated by enforcement agencies as a minor administrative step necessary for investigation. But for citizens, especially those living paycheck to paycheck, it can be a human crisis disguised as a technical procedure. The disruption of dignity, routine, financial independence, and personal credibility collectively transforms a procedural irregularity into a profound human rights concern. Without structured oversight, clear notice requirements, and accessible remedies, the system risks punishing the innocent in the very process of trying to protect society from cybercrime.

X. COMPARATIVE ANALYSIS

A. FREEZING PROCEDURES IN THE UK, US, AND EU

1. United Kingdom

In the UK, freezing of bank accounts typically happens through tools like Account Freezing Orders (AFOs) under the Proceeds of Crime Act (POCA) and related anti-money laundering laws. These are not casual administrative steps; they are judicially supervised measures.

Key features:

- **Court involvement:** Investigators usually apply to a Magistrates' Court to obtain an AFO. The court examines whether there are reasonable grounds to suspect that the funds are proceeds of crime.
- **Time-bound orders:** AFOs are granted for specified periods (for example, up to 2 years) and can be reviewed, extended, or discharged.
- **Right of challenge:** The account holder has the right to appear before the court, challenge the freeze, and request variation (for basic living expenses, business operations, etc.).

So, while the UK is tough on financial crime, its system embeds judicial checks and structured opportunities to be heard, which reduces the chances of silent, indefinite freezing.

2. United States

In the US, freezing or "blocking" of bank accounts generally occurs.

- Criminal seizure warrants issued by courts,
- Civil forfeiture actions,
- Regulatory actions in serious fraud or money laundering cases.

Key aspects:

- **Judicial authorization:** Law enforcement agencies typically need a warrant, court order, or grand jury process to restrain assets, especially if they belong to someone not yet convicted.
- **Due process:** The US Constitution, through the Fourth and Fifth Amendments, requires that seizures be reasonable and that individuals receive due process of law before permanent deprivation of property.
- **Post-seizure remedies:** Affected persons can file motions to release or modify the seizure, and courts consider hardship, necessity, and the strength of the government's case.

While the US system has its own controversies (particularly around civil forfeiture), the central role of courts and the constitutional due process framework make it harder for front-line officers to freeze accounts purely on oral instructions or vague suspicion.

3. **European Union (EU)**

In the EU, freezing of funds is regulated through a combination of.

- National criminal codes,
- EU anti-money laundering (AML) directives, and
- Regulations related to terrorist financing, sanctions, and financial crime.

Common threads across EU jurisdictions:

- **Legal basis & documentation:** Freezing usually requires a formal decision or order—either judicial or from a competent authority acting under clearly defined legal frameworks.
- **Notification & reasons:** Individuals are generally notified of the freeze and the reasons, subject to limited exceptions (e.g., where notice would jeopardize a sensitive terrorism investigation).
- **Rights to review and appeal:** There are codified rights to contest freezing orders, including appeals to courts or independent tribunals.

The EU also focuses heavily on data protection and privacy, recognizing that financial surveillance must be balanced against individual rights under instruments like the EU Charter of Fundamental Rights.

B. SAFEGUARDS USED IN ADVANCED CYBERCRIME JURISDICTIONS

Across the UK, US, and the EU, some common safeguards stand out, even though their laws differ.

- **Judicial or Quasi-Judicial Involvement:** Account freezing is typically not a mere administrative action by the police. Courts, magistrates, or adjudicating authorities usually review the request, ensuring that suspicion is supported by evidence.
- **Written, Reasoned Orders:** Authorities must record clear reasons justifying why a particular account is being frozen. This makes the decision traceable, reviewable, and less prone to arbitrariness.
- **Notification to the Account Holder:** Except in rare, sensitive cases, the citizen is told that their account has been frozen, the legal basis, and the body responsible. This gives them a fighting chance to defend themselves.
- **Right to Challenge / Appeal:** Individuals can approach courts or tribunals to
    - contest the freeze,
    - request partial unfreezing for essential needs,
    - argue the lack of nexus with the alleged crime.
- **Time Limits and Periodic Review:** Freezing orders are often time-bound and subject to review. Authorities must periodically demonstrate that the freeze remains necessary.
- **Consideration of Hardship:** Courts and regulators in these jurisdictions often explicitly consider human consequences—such as the impact on a person's livelihood or a business's survival—when evaluating whether a freeze should continue.

C. LESSONS FOR INDIAN CYBER POLICING

India does not lack legal tools. What it often lacks is structured safeguards in practice. From the comparative perspective, several key lessons emerge.

1. Move from Informal Freezing to Formal Orders

In many Indian cases, bank accounts are frozen on the basis of informal letters or emails from police to banks, sometimes even orally conveyed.

The UK/EU experience suggests that:

- Freezing should take place through formal, standardized orders,
- Orders should be reasoned, documented, and signed by responsible officers,
- Banks should not act on vague or undocumented requests.

This would reduce ambiguity and make it easier for citizens to understand and challenge the action.

2. Strengthen Judicial Oversight and Time-Bound Review

Comparative jurisdictions show that judicial oversight is not a luxury—it is a necessity.

For India, this means:

- Strict enforcement of Section 102(3) CrPC's requirement to inform the Magistrate immediately.
- Clear time limits on how long an account can remain frozen without filing of charges or substantial progress.
- Mechanisms for periodic review, where police must justify continuation of the freeze.

This would prevent preventive action from morphing into indefinite, quasi-punitive deprivation.

3. Guarantee Notice and the Right to Be Heard

While investigations sometimes require temporary secrecy, the default approach should be transparency. Borrowing from EU and UK practices.

India could:

- Mandate that, except in exceptional cases, the account holder must be notified in writing of the freeze and the basic reasons.
- Create a structured process for the citizen to submit an explanation, documents, or representation showing legitimate transactions.

This would humanise the process, restore a sense of dignity, and align policing with principles of natural justice.

4. **Build Proportionality into the Process**

Advanced jurisdictions increasingly stress proportionality—that enforcement must not cause collateral damage disproportionate to the suspected offence.

For India, this means:

- Freezing only suspected amounts, not entire balances, unless strictly necessary.
- Allowing partial unfreezing for essential expenses: food, rent, medical emergencies, educational fees, or business continuity.
- Considering the economic status of the person—what is a technical inconvenience for a wealthy account holder can be a survival crisis for a low-income worker.

Embedding proportionality would significantly reduce human suffering caused by overbroad freezing.

5. **Create Clear Administrative Redress Mechanisms**

In the UK/EU/US, individuals typically know where to go and what to file if they want to challenge a freeze: a court, tribunal, or regulator.

India can draw from this by:

- Establishing dedicated grievance cells within Cyber Crime units for account freeze complaints.
- Requiring banks to share contact details and case references of the law enforcement authority responsible.
- Setting up standard operating procedures (SOPs) that define timelines, documentation, and escalation routes for citizens.

This would reduce dependency on High Courts for relief and make justice more accessible to ordinary people.

XI. REMEDIES AND ACCOUNTABILITY MECHANISMS

When a citizen's bank account is frozen—often abruptly and without explanation—the immediate instinct is confusion followed by anxiety. What most people do not realize is that Indian law provides multiple layers of remedies, from administrative representations to constitutional courts. Each remedy serves a unique purpose: some are meant to secure quick answers, others to restore rights, and still others to ensure that the police are held accountable when they overstep legal boundaries. This section explores these mechanisms in depth, presenting them not as abstract legal tools but as practical pathways for individuals caught in the crossfire of flawed cybercrime investigations.

A. REPRESENTATION TO THE CYBER CELL AND THE BANK

The first remedy lies not in the courtroom but directly with the institutions involved—the Cyber Cell and the bank. A citizen whose account has been frozen has the right to demand clarity. A written representation addressed to the Cyber Cell acts as a formal request for transparency. In this representation, the citizen can seek the basic information that should have been provided from the start.

- Why was the account frozen?
- Which case or complaint triggered it?
- What specific transaction or connection raised suspicion?
- And most importantly, what steps must be taken to resolve the issue?

For the bank, the representation serves a different purpose: ensuring accountability for their role in executing the freeze. The bank must disclose the authority that issued the freeze direction, along with the date and reference of the communication. Without this, the citizen is left unable to navigate further steps. By insisting on written replies and acknowledgement receipts, individuals create documentation that can later prove crucial in court.

Many victims of wrongful freezes recount being trapped in a bureaucratic loop in which the bank blames the police, and the police point back to the bank. A formal representation breaks this loop by compelling both sides to acknowledge the citizen's rights and to respond in writing. While this remedy may not immediately defreeze the account, it is an essential foundation upon which all subsequent remedies depend.

B. MAGISTRATE COURT REMEDIES UNDER CRPC

A powerful yet often under-utilized remedy is approaching the jurisdictional Magistrate. The law requires that whenever a bank account is frozen under police seizure powers, the action must be reported to a Magistrate for oversight. The Magistrate becomes the first judicial guardian of the citizens' rights. By filing an application before the Magistrate, the individual can challenge the freeze on procedural and substantive grounds. The citizen may argue that the police did not record reasons for the freeze, did not inform them of the action, or failed to establish any reasonable nexus between the account and the alleged offence.

The Magistrate has multiple options at this stage: they may order the complete defreezing of the account, allow partial release of funds for essential needs, require the police to justify their action in writing, or set time-bound conditions for continuation of the freeze. For many individuals who cannot afford lengthy High Court litigation, this remedy is not only accessible but also effective. It acts as a corrective mechanism when police fail to comply with procedure, ensuring judicial supervision without requiring higher-level intervention.

C. HIGH COURT WRIT PETITIONS UNDER ARTICLE 226

When administrative avenues fail or when the freezing order is blatantly unlawful, the High Court becomes the most powerful and decisive forum for remedy. Through a writ petition under Article 226, a citizen can directly assert that their fundamental and constitutional rights have been violated. High Courts across India have consistently taken a strong stance against arbitrary freezes.

They often step in when the police:

- freeze accounts without any registered FIR,
- ignore the requirement to inform the Magistrate,
- refuse to share reasons or documents with the citizen,
- fail to respond to representations,
- or allow the freeze to continue indefinitely.

In such circumstances, the High Court may order immediate defreezing, impose guidelines, or direct the police to act in accordance with due process. Importantly, High Courts do not merely provide relief—they reaffirm constitutional protections such as equality, property rights, and the right to livelihood. For individuals whose lives have been disrupted due to mechanical or misguided freezing, the High Court often becomes the final safeguard against procedural injustice.

D. HUMAN RIGHTS COMMISSION COMPLAINTS

While courts address legal violations, Human Rights Commissions address the human impact—loss of dignity, trauma, and livelihood. When freezing causes disproportionate hardship, citizens may approach the State or the National Human Rights Commission. These Commissions treat such matters as violations of the right to life with dignity. They have the authority to summon police officers, demand explanations, conduct inquiries, and even recommend compensation.

For vulnerable groups—students, gig workers, daily wage earners, migrants—the Commission becomes a crucial platform to highlight the human suffering inflicted by administrative opacity or negligence. Human Rights Commission proceedings also

push law enforcement agencies to reflect internally on whether their procedures balance security with humanity. These cases often catalyze broader institutional reforms by spotlighting patterns of misuse and systemic gaps.

E. DEPARTMENTAL ACTION AGAINST ERRING OFFICERS

Every police officer is bound not only by law but also by internal conduct rules. When officers freeze accounts recklessly—without legal authority, without documenting reasons, or without notifying the citizen—they may be liable for departmental action. Senior police officials, including the Superintendent or Commissioner, can initiate internal investigations. These can result in warnings, written reprimands, transfers, suspension, or even disciplinary proceedings.

Citizens can trigger such accountability by filing a detailed complaint with senior officials or the state's Home Department. This remedy is crucial because it addresses the root of the problem: procedural misuse by individual officers or entire cyber units. When officers face consequences, it deters others from exercising freezing powers casually or mechanically. It encourages a culture of caution, documentation, and respect for citizen rights.

XII. NEED FOR REFORM

The increasing reliance on digital banking and online transactions has created a complex challenge for law enforcement: how to act swiftly enough to prevent cyber fraud while ensuring that innocent citizens are not harmed in the process. The current system of bank account freezing, however, often leans heavily toward investigative convenience at the expense of transparency, due process, and individual dignity. Reform is therefore not optional—it is essential. The following areas outline how cyber policing can evolve into a more accountable, humane, and constitutionally compliant institution.

A. SUGGESTED STANDARD OPERATING PROCEDURES (SOPS) FOR CYBER CELLS

There is an urgent need for uniform, legally grounded SOPs for Cyber Cells across India. Presently, practices vary from state to state and even officer to officer. Some

freeze accounts only after due inquiry; others issue broad freezing requests based on digital traces without verifying the legitimacy of each account.

A standardized SOP should include:

- A clear step-by-step procedure for when and how freezing orders may be issued.
- Minimum evidentiary requirements before freezing.
- Mandatory documentation formats for recording reasons.
- A checklist requiring officers to demonstrate nexus between the suspicious transaction and the alleged offence.
- Protocols to ensure freezing is targeted, not blanket in nature.

Such SOPs would reduce impulsive, arbitrary, or fear-driven decisions and create a consistent national standard that balances investigative needs with citizen protections.

B. MANDATORY NOTICE AND HEARING MECHANISMS

One of the most human deficiencies in current cyber policing practices is the absence of communication. Citizens often learn about the freeze through failed transactions rather than official notification.

Reform must introduce a mandatory notice framework, requiring that:

- The account holder is informed in writing as soon as the freeze is executed,
- The basic reasons or suspicion behind the freeze are disclosed,
- The citizen is given a timeline for response, and
- A hearing mechanism is created where individuals may submit explanations or supporting documents.

This notice need not compromise the investigation. Even a brief, structured notice protects dignity and allows citizens to demonstrate innocence before financial paralysis sets in. Hearing mechanisms also reduce reliance on courts, allowing administrative correction where errors occur.

C. PERIODIC REVIEW OF FREEZING ORDERS

A freezing order is meant to be a temporary investigative measure, not an indefinite punishment. Yet in practice, many freezes continue for months—or even years—without review. This leads to severe livelihood disruption even when the citizen is never formally accused. A reform-oriented framework must incorporate periodic judicial and administrative review.

Ensuring that:

- Police justify the continuation of the freeze at regular intervals—e.g., every 30 or 60 days.
- Magistrates or supervisory officers assess whether the legal grounds still exist.
- Cases with no progress are flagged for defreezing.
- The scope of the freeze is revisited to ensure proportionality.

By introducing review cycles, the system can prevent financial paralysis caused by outdated or forgotten freezing orders.

D. ENHANCED TRANSPARENCY AND TRACEABILITY

Transparency is the antidote to arbitrariness. A transparent system empowers citizens and disciplines institutions.

Reforms should mandate:

- That all freezing orders be logged in a secure, digital, traceable system accessible to authorized stakeholders.
- That banks provide citizens with clear information about which authority froze their account and how to contact that authority.
- That Cyber Cells maintain internal digital logs documenting the decision-making process behind each freeze.

Traceability would help identify patterns of overreach, deter misuse of power, and provide citizens with a clear roadmap to challenge or inquire about the freeze.

Transparency also reduces miscommunication between banks and police, ensuring faster resolution of wrongful actions.

E. STRENGTHENING CITIZEN REDRESSAL MECHANISMS

One of the most painful aspects for innocent individuals is the absence of accessible redressal routes. Most do not know whom to approach, how to submit representations, or whether the freeze is even legally justified. Reform must focus on creating strong, citizen-friendly redressal pathways.

Such as:

- Dedicated grievance desks at Cyber Crime Stations for account freeze issues.
- Standard timelines within which responses must be provided.
- Online portals where citizens can track the status of their freeze, upload documents, and receive official replies.
- Clear guidelines for banks outlining how much information they must provide to the account holder.
- Training programs for officers on human rights, due process, and proportionality.

Such mechanisms reduce dependency on courts and prevent routine matters from becoming constitutional crises. They also humanise law enforcement by acknowledging that even unintentional procedural lapses can deeply harm ordinary people.

XIII. CONCLUSION

A. SUMMARY OF FINDINGS

The study reveals a troubling gap between the intended legal safeguards surrounding bank account freezing and the reality experienced by citizens during cybercrime investigations in India. While the law requires reasonable suspicion, documentation, Magistrate oversight, notice to affected persons, and adherence to constitutional guarantees, these safeguards are frequently bypassed in practice.

The research shows that many freezes occur without an FIR, without notice, and without judicial reporting—leaving citizens financially incapacitated and emotionally distressed. Accounts are often frozen mechanically, sometimes in bulk, based on digital trails that are not individually scrutinized. The absence of clear Standard Operating Procedures (SOPs), inconsistent practices across states, and lack of administrative remedy pathways force citizens toward costly and time-consuming legal battles, often in High Courts, just to regain access to their own money. Across the cases, comparative jurisdictions, and lived experiences examined, one theme consistently emerges: procedural irregularity is not merely a technical flaw; it is a human rights concern with real social and economic consequences.

B. BALANCING CYBERSECURITY AND CIVIL LIBERTIES

Cybersecurity is undeniably a legitimate and urgent public interest. As digital transactions multiply and cyber fraud evolves, law enforcement requires the ability to act swiftly to prevent dissipation of funds. Yet, speed cannot come at the cost of constitutional discipline. A democratic society must ensure that security measures do not silence due process, and efficiency does not overshadow fairness. The challenge is not to choose between combating cybercrime and safeguarding civil liberties but to integrate both into a coherent and balanced framework.

This means adopting practices where:

- Suspicion is evaluated with care and supported by documented reasoning.
- Restrictions on financial autonomy are proportionate and time-bound.
- Citizens are informed, heard, and respected as rights-bearing individuals.
- Judicial oversight acts as a safeguard, not an afterthought.

The comparative analysis shows that advanced jurisdictions achieve both objectives—effective cybercrime control and strong procedural protections—indicating that India can, too. What is needed is not new laws, but better implementation of existing ones, anchored in constitutional morality.

C. RECOMMENDATIONS FOR POLICY AND PRACTICE

Reforms must be multi-layered, practical, and sensitive to the realities of both investigators and citizens. The following recommendations offer a path toward a fairer and more accountable system.

- **Creation of Clear SOPs:** Cyber Cells should operate under standardized guidelines outlining when and how freezes may be issued, with mandatory templates for recording reasons and demonstrating nexus with the alleged offence.
- **Mandatory Notice and Opportunity to Respond:** Citizens must be informed promptly of freezes, provided reasons, and offered a channel to clarify legitimate transactions. Even brief notices protect dignity and transparency.
- **Periodic Judicial and Administrative Review:** Freezing orders must not run indefinitely. Regular review—every 30 to 60 days—should assess necessity and proportionality, preventing prolonged hardship.
- **Proportional Freezing of Funds:** Instead of freezing entire accounts, only the disputed amount (or a capped value) should be restrained unless stronger justification exists. This approach protects livelihood while preserving evidence.
- **Enhanced Transparency and Traceability:** Banks and Cyber Cells must maintain digital logs of freezing orders accessible to senior officials and auditable bodies. Citizens should be able to track the status of their freeze and know which authority issued the order.
- **Strengthened Redressal Mechanisms:** Dedicated grievance cells, response timelines, online tracking systems, and citizen-friendly communication channels can reduce dependence on High Courts and create accessible remedies.
- **Officer Training and Accountability:** Training programs on due process, proportionality, human rights, and digital evidence assessment should be

mandatory. In cases of misuse or negligence, officers must face departmental scrutiny to ensure institutional integrity.

D. CLOSING REFLECTION

As India advances deeper into a digital future, the responsibility of the State is not only to pursue cybercriminals but also to protect the rights and dignity of its citizens. A freeze on a bank account may appear to be a procedural step, yet for the person affected, it can shatter financial stability, personal credibility, and mental peace.

A system that values both security and humanity is not just desirable—it is essential. Reforming cyber policing is not about weakening enforcement; it is about strengthening trust. When citizens feel protected rather than targeted, cooperation improves, investigations become more effective, and justice becomes not just a principle, but a lived reality.

XIV. REFERENCES

- Brown, C. S. D. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology. 9(1), 55-119.
- Bryant, R., & Kennedy, I. (2014). Investigating Digital Crime. In: R. Bryant and S. Bryant (Eds.), Policing Digital Crime (pp. 123-145). England: Ashgate.
- Bryant, R., & Stephens, P. (2014). Policing Digital Crime: The International and
- Organisational Context. In R. Bryant and S. Bryant (Eds.), Policing Digital Crime (pp. 111-121). England: Ashgate.
- Chang, L.Y.C. (2013). Formal and Informal Modalities for Policing Cybercrime Across the Taiwan Strait. Policing & Society, 23(4), 540–555.
- Gottschalk, P. (2010). Policing Cyber Crime. Retrieved from www.bookboon.com.

- Halder, D., & Jaishankar, K. (2016). Policing Initiatives and Limitations. In: J. Navarro, S.
- Clevenger, and C. D. Marcum (eds.), The Intersection between Intimate Partner Abuse,
- Technology, and Cybercrime: Examining the Virtual Enemy (pp. 167 - 186). Durham, 6North Carolina: Carolina Academic Press.