BEHAVIOURAL FORENSICS IN CYBERCRIME INVESTIGATION: A DOCTRINAL STUDY OF THE PSYCHOLOGY OF CYBER CRIMINALS

Vasundhara V K, BBA, LLM (Business Law),
Tamilnadu Dr. Ambedkar Law University, Chennai

Kaviya R, B.A, LLM (Cyber Law), Advocate, Madras High Court.

ABSTRACT

Cybercrime has become a global concern, with perpetrators crossing borders with ease and hiding behind anonymity. Investigations typically focus on technical artifacts such as logs, metadata, and device images, but these materials rarely explain why an offense was committed or help establish the mental element required for criminal liability. International measures, such as the Budapest Convention on Cybercrime (2001), have mostly focused on technological cooperation and the exchange of digital evidence. However, technological proof typically points to a device or account rather than the individual who created it. Behavioral forensics, which investigates an offender's motivations, routines, and patterns of behavior, is gaining popularity around the world as a supplement to digital investigation. The main contention is that behavioral analysis is an essential addition to technical forensics. Targeting decisions, weapon selection, timing, communication patterns, and operational security routines all reveal the motivations of offenders, including money, ideology, retaliation, and thrill-seeking, as well as characteristics like lack of self-control, narcissism. When properly analyzed, these traces can help identify insider threats, prove intent and mens rea, and support attribution. The methodology used in the study is doctrinal. The Information Technology Act of 2000, the Bharatiya Nyaya Sanhita of 2023, the Bharatiya Sakshya Adhiniyam of 2023, pertinent court rulings, and international agreements like the Budapest Convention on Cybercrime are among the key materials that are critically analyzed as primary sources. Scholarly works in criminology, forensic psychology, and digital forensics specifically, Routine Activity Theory, Social Learning Theory, and Neutralization Theory are examples of secondary sources. Although useful as an investigative tool, the study argues that behavioral analysis lacks explicit statutory acknowledgment and a clear admissibility criterion in court of law. It comes to the conclusion that a fair and efficient cybercrime investigation requires a balanced framework that protects constitutional rights while allowing the organized use of behavioral evidence in cyber forensics.

Keywords: Behavioral forensics, digital forensics, forensic psychology, digital investigation, digital evidence.

CHAPTER 1: INTRODUCTION

1.1 Background

Digital forensics has evolved into a field focused on the identification, preservation, analysis, and presentation of electronic evidence[1]. Its focus is mostly technical: it determines what happened on the system and when. Criminal responsibility, however, necessitates proof of who behaved and in what state of mind. Cybercrimes such as hacking, phishing, identity theft, and ransomware are generally perpetrated remotely and behind anonymizing technologies, widening the gap between a digital artifact and a responsible human[2]. Behavioral forensics analyzes an offender's online behavior, including target selection, tool choice, timing, language, and operational security, to determine their identity, purpose, and intent[3]. The 2023 overhaul of Indian criminal law through the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS), and the Bharatiya Sakshya Adhiniyam (BSA), as well as the Information Technology Act of 2000 (IT Act), provides an opportunity to examine where behavioral evidence fits within the legal architecture[4]

1.2 Statement of Problem

The IT Act and the new criminal laws do not govern behavioral profiling or set criteria for its dependability, despite the fact that investigators are increasingly deriving intention and identities from digital behavior. The two issues are whether behavioral analysis of cybercriminals is a legitimate investigative technique from a scientific and legal standpoint and whether Indian legal system and constitutional laws can support it without jeopardizing the right to privacy, a fair trial, and protection from self-incrimination.

1.3 Objectives

1. To investigate the idea, development, and theoretical underpinnings of cybercriminals'

[1] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3d ed. 2011).
[2] Majid Yar, *The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory*, 2 Eur. J. Criminology 407 (2005).
[3] Marcus K. Rogers, *The Role of Criminal Profiling in the Computer Forensics Process*, 22 Computers & Sec. 292 (2003).
[4] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India) [hereinafter IT Act]; Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) [hereinafter BNS]; Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India) [hereinafter BNSS]; Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India) [hereinafter BSA].

psychology.

2. To evaluate behavioral analysis as a research instrument and pinpoint its limitations.

3. To examine the national and international legal systems that control cybercrime investigations.

4. To assess behavioral evidence's admissibility, evidentiary value, and constitutional protections.

5. To compare Indian law to the legal systems of the USA, the United Kingdom, and Europe and to suggest changes.

1.4 Methodology

The research is comparative, analytical, and doctrinal. Statutes, court rulings, and international agreements are examples of primary sources. Books, peer-reviewed papers, and law commission findings in the fields of criminology, forensic psychology, and digital forensics are examples of secondary sources. In order to extract applicable lessons for India, the comparative component looks at a few chosen jurisdictions.

1.5 Hypothesis

Null Hypothesis (H_0): The current legal framework allows for the use of behavioral forensics in cybercrime investigations without the need for explicit legislative recognition.

Alternative Hypothesis (H_1): The current legal framework fails to adequately address the use of behavioral forensics in cybercrime investigation. The lack of clear standards on admissibility, procedure, and safeguards undermines both the efficiency of investigation and the protection of the accused's rights.

1.6 Research Gap

Legal study on electronic evidence, technical literature on digital forensics, and criminological research on cyber criminals have all emerged substantially independently. To the best of the author's knowledge, there isn't any doctrinal examination of how behavioral evidence interacts with constitutional guaranties, the BSA, and the BNSS in India. That gap is filled in this study.

CHAPTER II: CONCEPT AND EVOLUTION WITH THEORIES

The methodical examination of an offender's behavior as documented in digital traces in order to make conclusions regarding identity, motive, capability, and purpose is known as behavioral forensics. The idea that intrusions carry the stamp of the person behind them led to the adaption of offender profiling to computer crime, which has its roots in violent crime investigations.[5]As a result, the field's perspective on cybercrime has shifted from being tool-centered to seeing the perpetrator as a decision-maker reacting to opportunity.[6]There are a number of hypotheses that explain why crime happens and what evidence it leaves behind. According to Routine Activity Theory, crime happens when a motivated criminal meets a suitable victim without an adequate guardian; cyberspace expands targets and undermines guardianship[7]

Social Learning Theory describes how attitudes and techniques that are conducive to crime are learned through association, as evidenced by shared tools and forum participation.[8]

According to the Self-Control Theory, impulsivity and risk-taking are characteristics that might lead to negligent operational security.[9] Neutralization Theory demonstrates how criminals justify violence, such as by disputing victimization or injury, and these justifications frequently show up in chat logs.[10] Because of identity flexibility and dissociation anonymity, persons who conceal criminal behavior in physical space may exhibit it online, according to Space Transition Theory [11], which is supported by the online disinhibition effect.[12] Research on the Dark Triad of psychopathy, Machiavellianism, and narcissism provides further dimensions, however their predictive validity for any particular person is still debatable[13] Lastly, attribution is impacted by the norms, status hierarchies, and skill transfer that are shaped by hacker subcultures.[14] These ideas are not proof; rather, they are explanatory frameworks. Their ability

[5] Marcus K. Rogers, *A Two-Dimensional Circumplex Approach to the Development of a Hacker Taxonomy*, 3 Digit. Investigation 97 (2006).
[6] Yar, *supra* note 2.
[7] Lawrence E. Cohen & Marcus Felson, *Social Change and Crime Rate Trends: A Routine Activity Approach*, 44 Am. Socio. Rev. 588 (1979).
[8] Ronald L. Akers, Social Learning and Social Structure: A General Theory of Crime and Deviance (1998).
[9] Michael R. Gottfredson & Travis Hirschi, A General Theory of Crime (1990).
[10] Gresham M. Sykes & David Matza, *Techniques of Neutralization: A Theory of Delinquency*, 22 Am. Socio. Rev. 664 (1957).
[11] K. Jaishankar, *Space Transition Theory of Cyber Crimes*, in Crimes of the Internet 283 (Frank Schmalleger & Michael Pittaro eds., 2009).
[12] John Suler, *The Online Disinhibition Effect*, 7 CyberPsychology & Behav. 321 (2004).

[13] Delroy L. Paulhus & Kevin M. Williams, *The Dark Triad of Personality: Narcissism, Machiavellianism, and Psychopathy*, 36 J. Rsch. Pers. 556 (2002).
[14] Thomas J. Holt, *Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant*

to provide testable hypotheses about an offender which must thereafter be supported by independent technical evidence is what gives them their forensic significance.

CHAPTER III: BEHAVIOURAL ANALYSIS AS AN INVESTIGATIVE TOOL

Digital footprints are used in behavioral analysis. Information regarding working hours, language, talent, and preferences can be found via logs, timestamps, browser histories, metadata, conversations, and malware code. Modus operandi, the taught technique that changes with experience, and signature, the psychologically motivated component that tends to endure between offenses, are relevant distinctions.[15] Recurring targeting patterns, shared signatures, and coding quirks can connect offenses and identify a common offender.[16]

There are five main uses for behavioral analysis. First, by reducing the number of potential perpetrators, it facilitates attribution and suspect prioritization. Second, it aids in establishing knowledge and intent: planning and awareness of wrongdoing may be demonstrated by reconnaissance, preparation, the use of anonymizing tools, and the deletion of logs. Third, by spotting departures from an employee's typical behavior, it helps discover insider threats.

Fourth, as long as participation is voluntary, it influences interview technique by enabling questions to be framed around motive and justification. Fifth, by demonstrating the rationale behind the selection of certain targets, it promotes victimology and prevention.

The restrictions are substantial. Investigators are susceptible to confirmation bias; tools and stolen source code are widely circulated; datasets are tiny; verified base rates are hard to come by; and offenders may place false flags or imitate other actors. Therefore, digital evidence has to be weighed against mistake and other causes.[17] As a result, a behavioral profile should not be regarded as substantial proof of guilt but rather as an investigative lead that directs investigation.

CHAPTER IV: LEGAL FRAMEWORK

4.1 International

Although behavioral evidence is not specifically regulated by any international treaty, a number

Subcultures, 28 Deviant Behav. 171 (2007).
[15] Brent E. Turvey, Criminal Profiling: An Introduction to Behavioral Evidence Analysis (4th ed. 2011).
[16] Rogers, *supra* note 3.
[17] Casey, *supra* note 1.

of them influence the context in which it is collected. Subject to the protections in Article 15, the Budapest Convention makes unauthorized access, interference, device abuse, computer-related fraud, and forgery illegal. It also grants procedural authorities for accelerated preservation, production orders, search and seizure, and traffic data collecting[18]. Direct collaboration and electronic evidence disclosure are strengthened by its Second Additional Protocol[19]. The international framework is expanded by the 2024 adoption of the United Nations Convention on Cybercrime[20]. Directive 2013/40/EU harmonizes information system offenses within the European Union.[21] These tools make it easier to get the artifacts that are necessary for behavioral inference across borders, but they leave the assessment of behavioral opinion to local legislation. The Budapest Convention, to which India is not a member, makes collaboration and access to evidence kept elsewhere more difficult.

4.2 National

The IT Act has extraterritorial reach under section 75 and penalizes identity theft (section 66C), cheating by personation utilizing a computer resource (section 66D), and unauthorized access and damage (sections 43 and 66). Section 69 governs interception, while Section 79A permits Examiners of Electronic Evidence to be notified.[22] The BNS demands culpable mental states: personation is covered separately in section 319, and cheating under section 318 is based on dishonest or fraudulent inducement, therefore intent must be demonstrated.[23] The BNSS permits the production of documents and devices (section 94) and mandates forensic investigation at the scene for offenses carrying a sentence of seven years or more in prison (section 176(3)).[24] The BSA requires a certificate for electronic records (section 63), accepts expert opinion (section 39), considers purpose and behavior significant (part 6), and recognizes electronic records as papers.[25] The Digital Personal Data Protection Act, 2023 governs the processing of personal data, however section 17 exempts processing for the prevention,

[18] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, arts. 2–8, 14–21.
[19] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, May 12, 2022, C.E.T.S. No. 224
[20] G.A. Res. 79/243 (Dec. 24, 2024) (United Nations Convention against Cybercrime).
[21] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems, 2013 O.J. (L 218) 8.
[22] IT Act, *supra* note 4, §§ 43, 66, 66C, 66D, 69, 75, 79A
[23] BNS, *supra* note 4, §§ 318–319.
[24] BNSS, *supra* note 4, §§ 94, 176(3).
[25] BSA, *supra* note 4, §§ 6, 39, 63.

detection, or investigation of offenses[26]

Behavioral profiling is not covered by any of these clauses. There is no legal need for certifying a behavioral analyst, verifying a technique, or revealing mistake rates; instead, basic expert testimony principles are used.

CHAPTER V: ADMISSIBILITY, EVIDENTIARY VALUE AND CONSTITUTIONAL SAFEGUARDS

Each of the two layers of evidence used in behavioural analysis has its own set of admissibility guidelines. The underlying electronic record is the first. A certificate is required in order to permit computer output under section 63 of the BSA.[27] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal reiterated the Supreme Court's ruling in Anvar P.V. v. P.K. Basheer that secondary electronic evidence is inadmissible without the certificate, making it clear that the certificate is not necessary when the original device is produced.[28] [29] Thus, behavioural inferences based on uncertified records are susceptible. The analyst's opinion, which typically enters as expert testimony under section 39 of the BSA, makes up the second layer.[30] Indian courts consider expert opinions to be advisory, demand that their foundation and logic be revealed, and typically look for confirmation.[31] There is uneven judicial scrutiny of behavioral methods in India because the country has not formally adopted a reliability test like the one in Daubert. Additionally, profile evidence can lead to an unlawful inference of guilt based on similarity to a type. According to section 6 of the BSA, behavioural findings are the most suitable way to demonstrate motive, preparation, and conduct. [32] Since many cyber cases rely on circumstantial evidence and motive is neither required nor sufficient for conviction, the guidelines in Sharad Birdhichand Sarda v. State of Maharashtra applies: the facts must be proven beyond a reasonable doubt and create a chain of events that clearly indicates guilt. [33] A behavioural profile is unable to fill in a gap.

Constitutional protections limit the amount that can be collected. The Supreme Court ruled in

[26] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act], § 17.
[27] BSA, *supra* note 4, § 63.
[28] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).
[29] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).
[30] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).
[31] BSA, *supra* note 4, § 39.
[32] State of H.P. v. Jai Lal, (1999) 7 S.C.C. 280 (India).
[33] BSA, *supra* note 4, § 6.

Selvi v. State of Karnataka that, in the absence of voluntary consent, mandatory narcoanalysis, polygraph, and brain mapping tests violate Articles 20(3) and 21.[34] As a result, forced psychological testing of suspects is prohibited, while the distinction between testimonial coercion and material evidence made in State of Bombay v. Kathi Kalu Oghad is more closely aligned with the analysis of voluntarily generated digital footprints.[35] According to Justice K.S. Puttaswamy v. Union of India, informational privacy necessitates that state intrusion meet the requirements of legality, legitimate aim, and proportionality.[36]

In Anuradha Bhasin v. Union of India, restrictions on internet use were assessed against the principle of proportionality.[37] The procedural safeguards required for telephone tapping in PUCL v. Union of India also provide guidance for large-scale monitoring.[38] Broad exemptions under section 17 of the DPDP Act may allow behavioural profiling to proceed without meaningful oversight, while profiling based on proxies such as language, region, or religion may also raise concerns under Article 14.[39]

CHAPTER VI: COMPARATIVE ANALYSIS

America: The Federal Rule of Evidence 702 governs expert testimony, and the reliability inquiry in Daubert v. Merrell Dow Pharmaceuticals, Inc. extended to non-scientific expertise in Kumho Tire Co. v. Carmichael[40] [41] [42] In general, courts are hesitant to accept profile evidence that is offered to demonstrate that an accused person fits a criminal type. Rules 901 and 902(13) – (14), which permit self-authentication through certification, facilitate the authentication of electronic records.[43] As demonstrated in Riley v. California and Carpenter V. United States, the Fourth Amendment restricts digital searches[44] [45] The Computer Fraud and Abuse Act is the main offense statute.[46]

[34] Selvi v. State of Karnataka, (2010) 7 S.C.C. 263 (India); India Const. arts. 20(3), 21.
[35] State of Bombay v. Kathi Kalu Oghad, A.I.R. 1961 S.C. 1808 (India).
[36] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
[37] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[38] People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).
[39] DPDP Act, *supra* note 27, § 17; India Const. art. 14.
[40] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993).
[41] Fed. R. Evid. 702.
[42] Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).
[43] Fed. R. Evid. 901, 902(13)–(14).
[44] Riley v. California, 573 U.S. 373 (2014).
[45] Carpenter v. United States, 585 U.S. 296 (2018).
[46] Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

United Kingdom: In R v. Turner, the court held that expert evidence is inadmissible on matters within ordinary human experience, limiting psychological opinions about typical behaviour.[47] The Law Commission's recommendation for a statutory reliability test for expert evidence informed subsequent procedural reforms[48]Section 78 of the Police and Criminal Evidence Act 1984 permits the exclusion of unfair evidence, while the Computer Misuse Act 1990 principally governs cyber offences.[49]

European framework: Only automated decisions based on profiling are prohibited by the General Data Protection Regulation and the Law Enforcement Directive, which also mandate protections when such processing is employed.[50] [51] According to S. and Marper v. United Kingdom, Article 8 of the European Convention on Human Rights requires that personal data be used and retained proportionately. [52]

Indian lessons: A reliability gate for expert testimony, restrictions on type-based profile evidence, and statutory data-protection safeguards on profiling are the three ways that jurisdictions handle behavioral evidence, according to the comparison. India only has the first overall, and the second and third only marginally.

CHAPTER VII: CONCLUSION AND SUGGESTIONS

According to this study, behavioral forensics enhances cybercrime investigations by facilitating attribution, intent, and prevention by linking technical artifacts to human decision-making. However, its methods are not standardized, its reliability is limited, and it is neither validated nor regulated by Indian law. Therefore, the alternative hypothesis that behavioral analysis is only useful when it is transparent, structured, and constrained by the constitution is strongly supported.

The following recommendations are made:

[47] R v. Turner [1975] Q.B. 834 (Eng.).
[48] Law Comm'n, Expert Evidence in Criminal Proceedings in England and Wales, Law Com No. 325 (2011) (U.K.).
[49] Police and Criminal Evidence Act 1984, c. 60, § 78 (U.K.); Computer Misuse Act 1990, c. 18 (U.K.).
[50] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data, 2016 O.J. (L 119) 1, art. 22.
[51] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities, 2016 O.J. (L 119) 89, art.11
[52] S. and Marper v. United Kingdom, 2008-V Eur. Ct. H.R. 213 (Grand Chamber).

- **Statutory guidelines:** The Union should issue binding standard operating procedures under the BNSS and the IT Act to govern the use of behavioural analysis in cyber investigations.

- **Investigative leads, not proof:** Behavioural reports should be treated as investigative leads. Courts should require corroboration through independent technical evidence.

- **Reliability disclosures**: Under section 39 of the BSA, experts should disclose their methodology, assumptions, error rates, and alternative hypotheses. Courts should also adopt a structured reliability inquiry.

- **Accreditation and training:** Forensic psychologists and examiners should be accredited, and investigators should be trained to recognize confirmation bias and false flags.

- **Rights-based safeguards**: Profiling should be subject to proportionality review, judicial oversight, data minimisation, and audits for discriminatory bias. The investigative exemption in the DPDP Act should also be narrowed.

- **International cooperation:** India should reassess its participation in the Budapest regime and the UN Convention to improve access to cross-border evidence.

- **Research and rehabilitation:** Validation studies, diversion pathways, and ethical-hacking initiatives should be supported so that psychological insight can also contribute to prevention.

An ethically bounded framework could strengthen prosecutions, protect individual rights, and establish behavioural forensics as a credible component of cybercrime investigations in India.