CYBERCRIMINAL PROFILE AS AN EXPERT EVIDENCE IN A COURT OF LAW - THE NEED OF THE HOUR

Deepikka R S, Research Scholar, School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Chennai.

ABSTRACT

After the COVID pandemic, the trend in the criminal culture has shifted towards cybercrime, the rate of which has sharply raised in the past few years, as opposed to the decline in traditional crimes. Unlike traditional crimes, the process of identification, arrest, investigation, evidence collection and conviction in cybercrime is very difficult, due to its inherent character traits like transborder jurisdiction issues, lack of international cooperation, difficulties in attribution etc. In 2022, the rate of cybercrimes increased by 24% as compared to 2021[1]. The estimated global expenditure or loss due to cybercrime is approximately10.5Trillion$ US in 2025[2], but the rate of arrest and conviction in such a serious crime in very miniscule in India. In the traditional criminal investigation, the law enforcement has used the science of criminal profiling, the tool with the combines the merits of multidisciplinary sciences like criminology, psychology and forensics, to draw the character and psychological profile of an offender that makes it easy to identify and prosecute him. However, this method has had different levels of success in identifying the criminal and as evidence in the Court of law. Adoption of this method in cyber jurisprudence is in its nascent stage and its adoption is an immediate necessity as technology can only trace a crime back to a system or device and not directly to the perpetrator, which may be a loop hole used by defence to secure acquittal. This paper suggest the adoption of criminal profiling in the cyber jurisprudence with adequate scientific standards, data driven, based on the experience of the profiler to generate admissible expert evidence that facilitates not only the identification of the criminal but also to bring them to justice in the Court of law.

Keywords: cybercriminal profiling, psychology, criminology, digital forensics, expert evidence.

[1] National Crime Records Bureau, Report on Crime in India 2022 Statistics: Volume II (2023), *available at:* https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf,(Last visited on Feb 20, 2024).

[2] Steve Morgan, "Cybercrime to Cost the World 10.5 trillion Annually by 2025", Cybercrime Magazine (2020), *available at:* https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (Last visited on Dec 04, 2023).

INTRODUCTION

Cybercriminal profiling is slowly gaining attention from the Western criminologists due to the unprecedented rise in cybercrimes[3]. It is analogous to traditional criminal profiling methodology, but presents new kinds of challenges to investigators due to the nature of cybercrimes, like jurisdictional issues and difficulties in collecting evidence. The Information Technology Act, 2000 read with Bharatiya Nyaya Sanhita, 2023, extends their long arm and exerts the jurisdiction of Indian Courts on cybercriminals anywhere in the globe, if any Indian computers or citizens are subject to attack[4]. However, these provisions will not be useful if the law enforcement fails to identify the criminal in the first place.

Statistics show that arrests are made in only half the reported cybercrimes and only in 1.6% of those cases are there any convictions[5]. This might be because the police haphazardly arrested an innocent person or they got the real culprit but failed to achieve conviction due to lack of concrete evidence. This shows the incapacity of the criminal justice system to deal with technical crimes and seeking the help of a cybercriminal profiler might be a valuable solution for the issue.

Presently India is way behind in the research of criminal minds, especially the psyche of cybercriminals, which aids in identifying them and deterring future crimes. Cybercriminal profiling will aid the law enforcement in doing so, additionally if done in a reliable manner it could serve as an expert evidence in the court of law.

Thus, this paper proposes criminal profiling as a tool to identify criminals and bring them to justice. By conducting digital forensics of a digital crime scene the tools, modus and timeline is deduced, then psychological and criminological theories are applied on the details regarding crime scene characteristics, modus operandi and victimology to draw a profile for the offender. The research also aims to promote a scientific and effective hybrid profiling method to draw a reliable cybercriminal profile that can be used as corroborative expert witness in the Court of law to increase the conviction rate of cybercrimes in India.

[3] Arun Warikoo, "Proposed Methodology for Cybercriminal Profiling", *ISJ-GP* (2014), *available at:* https://www.tandfonline.com/doi/abs/10.1080/19393555.2014.931491, (Last visited on Dec 1, 2025).

[4] Section 1 and 75 of the Information Technology Act, 2000 (Act 21 of 2000), read with Sections 3 and 4 of Indian Penal Code, 1860 (Act 45 of 1860).

[5] Ministry of Home, "Cyber Crimes and Fraud*s*", (PIB, 2022), *available at:* https://www.pib.gov.in/PressRelese Detailm .aspx?PRID=1883066, (Last visited on Dec 1, 2025).

CYBERCRIMINAL PROFILING

Criminal profiling is an interdisciplinary science and intellectual art performed by subject matter experts from the fields of psychology, forensics, criminology, sociology and biology.

Criminal profiling can be defined as a scientific technique, used to analyse and assess a crime scene to construe the potential behavioural patterns and characteristics of the person who committed the crime[6]. The resultant report generated is termed as a criminal profile which has a potential to be used as a corroborative expert evidence in a court of law.

Drawing from the above, when a criminal profile is drawn to identify the motives, characteristics, personality traits of a cybercriminal, based on investigation of a cybercrime scene, the tools and techniques used digital footprints to pinpoint to him, rather than the device.

FACTS THAT CAN BE PROVED USING CYBERCRIMINAL PROFILING

The primary output a criminal profile can generate is a digital biography, which reveals the user's search patterns, e- mail id, usernames and passwords, the number of accounts, avatars and pseudonyms used in social media sites , IP address and its geo location which will establish their signature and link them to a crime[7]. The following are the potential outcomes of a well-drawn cybercriminal profile that can shed lights in various aspects of the cyber crime and the associated criminal:

a. The profile can trace his technical skills, technology-based education or expertise in a niche area, to narrow down the suspect pool and serve as corroborative evidence linking him to the cybercrime.

b. The amount of digital assets he possess, like virtual currency, pirated software, movie, music, pornography, illegal data etc, can serve as evidence against him.

c. If he is profiled to be an organised offender, it can help to establish his preplanning, and dishonest and fraudulent intention which is necessary to prove an offence under Section

[6] Gráinne Kirwan and Andrew Power, *The psychology of cybercrime*, (IGI Global publication, 1st edn., 2011).

[7] Chad M steel, "Idiographic Digital Profiling Behavioural Analysis Based On Digital Forensics", 9 *JDFSL* (2014), *available at:* https://commons.erau.edu/cgi/viewcontent.cgi?Article =1160&context=jdfsl, (Last visited on Dec 2, 2025).

66-66F and he cannot avail the exceptions of accident, coercion or mental illness.

d. If he had taken many counteractions like IP masking, encryption, using throwaway accounts, VPN or anonymisers intentionally, it can prove his intention to avoid detection and shows a guilty mind. This information can be shown to a magistrate to obtain a search warrant.

e. Based upon his sophisticated technical or criminal skills and use of resources the criminal's hierarchy in the group can be fixed, to see if he is the head or just a follower. This will change the course of his trial.

f. The time of the attack can help track the time zones and aid in geographical profiling. By combining it with special modes or tools used by the criminal, the crime can be narrowed down to a region of origin. For example, Russian cybercrime groups are notoriously known for hacking, North Korea is famous for surveillance, Chinese cyber spies are well known in espionage, Iran is well known for web defacement. This can help proving cyber warfare cases in International Criminal Court

g. Analysing the crime patterns will lead to finding a weak point where he broke his anonymity and forgetfully used his real identity. A best example is the slipup of 'Dread Pirates Roberts' as Ross Ulbricht which lead to his conviction in the Silk Road case[8].

h. A technical profile constructed based on the criminal's knowledge of the technical domain, will help categorise him as an expert or newbie. If he is an expert he might have been convicted previously and get enhanced punishment.

CRIMINOLOGICAL AND PSYCHOLOGICAL THEORIES OF CYBERCRIMES

A person's personality is developed based on a unique continuous and long-standing pattern of his emotions, thoughts and behaviour, that controls how he expresses his feelings and actions.[9]

Studies show that criminal behaviour, is a response to stresses like impulses, psychoneurotic

[8] UNODC SHERLOC database, available at: https://sherloc.unodc.org/cld/en/case-lawdoc/cybercrimecrimetype/usa/2017/united_states_of_america_v._ross_william_ulbricht_no._15-1815-cr_2d_cir._may_31_2017.html, (Last visited on Dec 1, 2025)

[9] Walter Mischel, "Toward an integrative science of the person", 55 *ARP*, 1-22 (2004), *available at:* https://www.annualreviews.org/content/journals/10.1146/annurev.psych.55.042902.130709 (Last visited on Dec 2, 2025).

reactions, subconscious motives, outburst of suppressed aggressions etc.[10] the following criminological theories not only outline the characteristics of a traditional criminal but can also be applies to study the psyche of a cyber criminal.

A. Rational Choice Theory

In cybercrime if the benefits outweigh the risk of getting caught, the criminal is likely to carry on the offence. For example, selling narcotic drugs in illegal dark web market place will yield millions of profits as evident in cases like Silk Road and Silk Road 2.0. and due to anonymity and lack of regulation there is less risk of getting caught, thus drug trafficking is still frolicking in dark web.

B. Deterrence Theory

He proposed that the penalties and sanctions must be certain (higher likelihood of getting caught), stringent (the punishment is intense enough to dissuade the criminal form attempting the crime) and speedy (sentences should be delivered swiftly and no delay of justice) to make the costs of doing crime outweigh the benefits, thereby deterring the criminal form engaging in it. Thus, to prevent a wannabe cybercriminal or restrict an experienced cybercriminal, it is paramount to create and enforce effective cyber laws and regulations with strict punishments and penalties which are certain, stringent and speedy.

C. Routine Activity Theory (RAT)

The theory states that, chance to commit criminal activities occurs conditional to the temporospatial conjunction of a motivated criminal, a suitable target, and absence of effective guardianship. The internet is favourable for the convergence of such motivated cybercriminals, their vulnerable victims, via chatrooms and social media and the non-existence of capable supervision or protection from law enforcement or even lax cyber security measures like not using anti-virus, cyber threat intelligence, anti-malware, firewall protection etc[11].

[10] John Douglas, Ann W. Burgess, *et.al., Crime Classification Manual: A Standard System for Investigating and Classifying Violent Crimes*, (Wiley, 2nd edn., 2006).

[11] Thomas J Holt and Adam M Bossler, "Examining the relationship between routine activities and malware infection indicators", 420–436 *JCCJ* (2013), *available at:* https://journals. sagepub.com/doi/10.1177/1043986213507401, (Last visited on Dec 2, 2025).

D. Self-Control Theory

This theory profiles criminals with low self-control to be impulsive, adventure seeking, having low tolerance to disturbance and frustration, self-centred and lacks diligence[12].

Petty cybercriminals frequently tend to do impulsive crimes like digital piracy, cyber harassment, cyber bullying and unauthorized access of computer resources. [13]

E. Gratification Theory

This theory proposes that people commit cybercrimes to fulfil some psychological desires or to attain gratification. For example, some criminals do cybercrime to gain power, control, or superiority over others, like cyber bullies and perpetrators of online sextortion.

F. General Strain Theory

This theory argues that when people face strain, they will feel negative emotions and as a coping mechanism they will do crime. In the cyberspace too, people experiencing such strain might relieve it by indulging in cybercrimes. For example, individuals facing financial strains may commit cyber financial frauds, online banking frauds, phishing, card frauds etc[14].

G. Anomie Theory

Anomie refers to a condition of social disintegration or normlessness[15]. The theory states that a person's participation in cybercrime might be his response to social isolation, frustration or marginalization.

[12] Alexander T. Vazsonyi, Jakub Mikuška, et.al., "It is time A meta-analysis on the self-control-deviance link", 48–63 *JoCJ* (2017), *available at:* https://www.sciencedirect.com/science/Article/pii/ S004723521630099X, (Last visited on Dec 3, 2025).

[13] Christopher M. Donner et al, "Low Self-Control and Cybercrime Exploring the Utility of the General Theory of Crime Beyond Digital Piracy", 165–172 *CHB* (2014), *available at:* https://libres.uncg.edu/ir/asu/f/Donner_Marcum_et%20al_2014_Low%20Self%20Control%20Cybercrime.pdf, (Last visited on Dec 2, 2025).

[14] Hyunseok Jang and Juyoung Song, "Does The Offline Bully-Victimization Influence Cyberbullying Behaviour Among Youths? Application of General Strain Theory", *Concepts in Human Behaviour*, 85–93 (2014), *available at:* https://www.researchgate.net/publication/259132252, (Last visited on Dec 2, 2025).

[15] "Psychological theories dealing with cybercrime Learning and Motivation", Centurion University (2020), *available at:* https://courseware.cutm.ac.in/wp-content/uploads/2020/06/Psychological-theories-dealing-with-cyber.docx., (Last visited on Dec 3, 2025).

H. Theory of Neutralization and Moral Disengagement Model

Few categories of cybercriminals like cyber terrorists, hacktivist, cyber spies and perpetrators of cyber war, really believe that they are working for the greater good and the victim deserves the punishment. By adopting such an attitude they able to do the crimes without guilt.

I. Social Learning Theory

It states that people learn to do criminal acts from social interactions, that support their criminality or by following role models, who have gained advantage by committing such crimes. People with low self-esteem pursue other criminal peers , to learn the art of crime from. who also strengthen their desire to commit crimes by rationalising and justifying it[16].

J. Space Transition Theory

It is the first criminological theory propounded specifically for cyberspace, by the Indian criminologist Dr. Jaishankar Karuppannan. The theory focuses on space transition, correlating the change in criminal's behaviour as he moves from physical world into the virtual world and claims that individuals act differently in both spaces and those who supressed criminal intentions in real world due to factors like their image or status, would have more inclination to express said criminal intentions and commit crimes in cyber space[17].

GENERAL PROFILE OF CYBER CRIMINALS

Based on the above theories I have drawn generic profiles for four types of cyber criminals affecting individuals, property, government, organisation and society, namely cyberbullying, cyber terrorism, hacking and cyber financial frauds.

	HACKER	**CYBER BULLY**	**FINACIAL FRAUD**	**CYBER TERRORIST**
Motive	Financial, ideological	Social dominance, fun	Financial gain, Greed	Political or religious dominance,

[16] George Higgins, Brian Fell, "Low Self-Control and Social Learning in Understanding Students' Intentions To Pirate Movies in The United States", *SSCR* 339–357 (2017), *available at:* https://psycnet. apa.org/record/2007-13516-003, (Last visited on Dec 3, 2025).

[17] Jaishankar Karuppannan, "Space Transition Theory Of cybercrimes", IJCC (2008), available at: https://www. cybercrimejournal.com/pdf/Editoriaijccjuly.pdf, (Last visited on Dec 1, 2025).

		seeking revenge		revenge and intolerance
Level of motivation	Very high	Medium motivation level	Very highly motivated	Very highly motivated
Organisational structure	Ranges from organised, community, state funded	Unorganised but persistent	Organised community.	Organised, state sponsored
Skill level	Highly advanced	Medium to high technological skills	Very high technical skills	High technical skills
Technicality and Character	Skilful, goal oriented	Aggressive, insensitive, need for control	Strategic planners, opportunist, manipulative	Radical, insensitive, misguided, brain washed
Choice of victim	Websites of Government organisations	known peer- for revenge or fun stranger- different ideology, race, religion.	Organisations with poor cyber security, Careless individuals, lacking digital and financial literacy.	Enemy nations and civilians with different political or religious ideology
Method of attack	Malware, virus, DDoS, Phishing, social engineering	Sending offensive messages through social media, chatrooms, anonymously	phishing, vishing, smishing, card frauds, ID theft etc.	Ransomware, Web defacement, attack on dams and power plants
Level and severity of attack	Very severe. Causes Financial, data and reputational loss	Severely damaging to victim especially emotionally	High financial and emotional damage to assets of victims,	Severely intense, causing heavy damage to person and property of victims

Table 1. General profile of 4 kinds of cybercriminals

LEGAL AND JUDICIAL ASPECTS OF CRIMINAL PROFILING IN INDIA

In the 21st century the Indian Courts have been advancing towards adopting new scientific evidences like DNA profiling and digital evidence, but have shown a restrictive mentality in admitting pseudo-scientific testimony. The Courts are vested with the duty and discretion to decide whether new forms of evidence, meets the conventional admission standards. The Courts have agreed that they have no doubt that offender profiling is very useful in crime investigations but the question remains whether Indian Courts would be open to admit it as evidence in a trial. The nature of criminal profiling makes it difficult for it to be subjected to reliable testing[18].So if criminal profiles are introduced in a trial supported with expert testimony of the profilers, the judges must make the key decision on its admissibility and weightage in deciding the case, keeping in mind it would serve as precedent for future cases [19].

By analysing the Indian judiciary's adaptability to new and scientific evidences, I believe the Courts have been broad minded in accepting the same. This attitude has been constant since the early 1970s, when in the case of **Shivaji Sahabrao Bobade v. State of Maharashtra[20]**, the Court stated that they will not disallow expert evidence merely because it involves a different science. It declared that "*Courts must have a scientific attitude, else it will be guilty of judicial superstition*". This stand point has continued over the decades as courts have continued to accept new age evidences in the form of DNA test, digital evidence from CCTV video footage, smart devices, Social media and e-mail messages, AI generated evidence, FRT etc. So there is a great chance that Courts will be open minded to admit a useful tool like criminal profiling.

On question of what new types of scientific methods of expert evidence can be admissible, The Supreme Court ruling in **Ranjitsinh Brahmajeetsinh Sharma v. State of Maharashtra[21]** is interesting to note. The Court whilst scrutinising the credibility and admissibility of a brain mapping test report held that, to become admissible a scientific test must be proved authentic, reliable and must have higher probative value. Thus only if a cybercriminal profile is scientific

[18] Norbert Ebisike, *Offender Profiling in the Courtroom The Use and Abuse of Expert Witness Testimony*, (Praeger Publishers, 1st edn., 2008).

[19] Scott Ingram, "If the profile fits admitting criminal psychological profiles into evidence in criminal trials", *JUCL* 239–266 (1998), *available at:* https://openscholarship.wustl.edu/ cgi/viewcontent.cgi?Article=1025, (Last visited on Dec 4, 2025)

[20] (1973) 2 SCC 793.

[21] (2005) 5 SCC 294.

and authentic and has probative value with respect to case in hand it shall be used as evidence.

Again in **Dharam Deo Yadav v. State of UP**[22], while expressing the significance of accepting new forms of scientific evidence, the Court stated that *"in this age of science, we have to build legal foundations that are sound in science and law. Practices and principles that served in the past, must give way to innovative and creative methods, if we want to save our criminal justice system".*

The Supreme Court in **State of Haryana v. Bhagirath,** observed that "*scientific advances necessitate a progressive approach towards the acceptance of expert testimony*", on condition that it fulfils established criteria like

a. It should not have prejudicial effect which makes the case unfair towards a party, or confuse the Court on the issue of case.

b. It should have a high probative value i.e. useful to reach a judgement in the trial.

c. The evidence must be derived from a credible source, legally.

d. It must be scientifically proven to be reliable.

e. The expert evidence must have direct relevance to the case in hand.

USE OF CYBERCRIMINAL PROFILING BY DEFENDENTS

Cybercriminal profile can act as a tool in the hands of the defence to crack any evidence introduced by the prosecution, especially in cases where law fixes reverse onus of proof on them. Articles 14, 20 and 21 of the Indian constitution guarantees fair trial, with a presumption of innocence of the offender until proven guilty, and fixing burden of proof on the prosecution.

It is especially useful in cases where the law fixes reverse burden of proof on the defendant. For example under Section 30 of the POCSO Act, 2012 a culpable mental state is presumed unless disproved **beyond reasonable doubt.** A person accused for possession of cyber or child pornography can call in an expert to prove that he doesn't fit the pattern of a usual criminal who consumes such material. Similarly, in case of financial frauds the FEMA Act, 1999,

[22] (2014) 5 SCC 509-C

presumes a culpable mind unless disproved and Section 24 of Prevention of Money Laundering Act 2002, fixes the burden of proving that the proceeds of crime as untainted property on the accused. In such cases the defendant can hire a forensic expert who collects digital data from his devices which can be analysed by a forensic psychologist to prove that he doesn't fit the pattern of a financial fraud.

The defence can use Cybercriminal Profiling as a tool to cause reasonable suspicion in the mind of the judges, that he could not have committed the crime or that someone else committed it. When the opinion of a profiler called as expert witness by the defence is corroborated by other factors like physical or digital evidence or alibis, the defendant's innocence can be established.

In this regard the judgement and opinion in the **Ajay Kumar Agarwal v. Union Territory of JK and Ors**[23] is relevant. Here the Court opined that to guarantee a fair investigation the IO must consideration all evidences both supporting and defeating his theory on the accused. Their investigation should not be one sided and focusing on only collecting facts that corroborate the allegations and ignoring others which crushes it. Thus, if an accused submits any document proving his innocence to the IO, he must accept it and consider it in investigation to bring out the real truth.

PROPOSED METHODOLOGY OF CYBER CRIMINAL PROFILING

The cybercriminal profiling methodology must take a holistic and multi-dimensional approach with collaborative efforts of the law enforcement, psychologist, criminologist and digital forensics experts. So a separate unit must be formed in the cyber cells comprising of all the above said experts to conduct cybercrime investigations. This special wing of the law enforcement, designated as the 'Cyber Profiling Unit' (CPU) will act as the heart of cybercrime investigating unit. The CPU must adopt a hybrid criminal profiling technique built on data and statistics supported by expert analysis to draw the profile of the criminal produce reliable evidence.

POTENTIAL BENEFITS OF ADOPTING THE PROPOSED METHODOLOGY

- Since it uses a multi-disciplinary model of criminal profiling, involving experts of criminology, psychology, digital forensics and law, the resultant report will create a

[23] WP(C) No. 821/2022 decided on May 12, 2022.

reliable evidence that would hold strong in a Court of law.

- This method will increase the rate of conviction of cybercrimes thereby creating fear in the minds of criminals that, the chance of being caught will increase and deterring new crimes. In the long run this might bringdown the rate of cybercrimes in India

- Similarly it will prevent repeat offenders, as they are aware that their data is already in the system and they will be quickly identified.

- This method can also be used by the defendant to prove their innocence by showing that they doesn't match the typical profile of the crime, especially in cases fixing reverse burden of proof on the defendant.

- Using this method, the investigation will not only end up with the device used for the attack but paints a picture of the culprit behind the device, his demographic and psychological characteristics so that he doesn't escape conviction.

- Thus it will help improve the efficiency in identification, arrest and conviction of cyber criminals.

- New kinds of evidence will aid in solving new age crimes which would otherwise be unsolvable and sees no justice served.

CONCLUSION

Cybercrimes are exponentially growing and will not stop anytime soon. Though India has many general and specialised laws to penalise cybercriminals along with numerous cyber cells to curb this menace, it is still uncontrollably flourishing. This is in part due to the fact that the criminal justice system struggles to identify and arrest the real criminal, and even if they do they find it difficult to produce enough evidence in a court to get a conviction. The Indian judicial system strongly believes the principle of "**Ei incumbit probatio qui dicit, non qui negat"** by which it always presumes a person to be innocent until they are proven guilty. But this should not deter the development of new scientific methods trying to bring the actual criminal to justice. One such method is the proposed cybercriminal profiling methodology.

21st century criminal investigations and trials mostly rely on new scientific methods. In recent years the Indian law enforcement has been adapting many new technologies like AI policing, CMAPS (Crime Mapping Analytics and Predictive System), Trinetra app[24] that uses AI to do facial recognition and tracking of criminals etc. So I argue that this is the correct time for the government to take percolate cybercriminal profiling as a policing technique that use technology and knowledge of experts to detect cybercriminals and produce the same as evidence in the court to ensure conviction.

This paper proposes that Investigating Officers work in tandem with the Cyber Profiling Unit (CPU) consisting of experts from fields like psychology, criminology, forensics and law. They shall follow a hybrid methodology to perform profiling to produce a report that contains the digital biography, socio demographic and psychological characteristics of the cybercriminal.

The resultant cybercriminal profile will be an effective evidence with high probative value and expert profilers can provide their testimony in the court to support the same.

The court have the duty towards the victim and the society to bring the criminal to justice. At the same time it must act as a gatekeeper of unreliable evidence that could end up prejudicial to the accused. Scholars believe that to solve complex disputes in a technologically forward society the courts must be open to technical advancements that facilitates solving such disputes.[25]

Cybercriminal profiling is the new age, holistic answer for the ever-growing menace of cybercrimes by quickly identifying and convicting them.

The motive of a cybercriminal may be anything ranging from money, greed, thrill, revenge, fun or hatred, but the aim of the criminal justice system is only one and that is to penalise the criminal and provide justice to the victim and the society. In my opinion cybercriminal profiling will act as the heart of cybercrime investigation and bring drastic increase in number of arrests and convictions and ultimately reduce the cybercrime rate in India. Hoping to see the Indian police and Courts welcoming this essential and novel methodology and propel India to become one of the safest countries in the cyber space and work towards cyber peace.

[24] AI is being used by the UP Police to catch criminals, IndiaAI (2019), *available at:* https://indiaai.gov.in/case-study/ai-is-being-used-by-the-up-police-to-catch-criminals, (Last visited on Dec 4, 2025).

[25] National Academy of Sciences, "Reference Manual on Scientific Evidence", (Federal Judicial Centre, 2011) *available at:* https://www.fjc.gov/sites/default/files/2015/ SciMan3D01.pdf, (Last visited on Dec 4, 2025).