International Journal of Enhanced Research in Educational Development, IJERED,
ISSN: 2320-8708, Vol. 13 Issue 2, Mar.-Apr, 2025

Relation between Science and Law

Dr. A. A. Kadeejabi

Associate Professor Department of Law, Government Law College, Thrissur, Kerala, India

ABSTRACT

This study examines how scientific advances improve justice and how legal systems encourage scientific research. It emphasises the importance of cybersecurity, forensic science, and digital evidence in law enforcement and justice. The research targets Indian judicial issues such restricted forensic infrastructure, insufficient digital evidence guidelines, and legal professionals' scientific literacy. Comparing India to the US shows it needs technology advances to compete globally. India should strengthen its forensic and cyber infrastructure, implement comprehensive digital and forensic evidence admissibility frameworks, and invest in specialised training for judicial and law enforcement professionals, according to the research. India's justice system could benefit from international collaboration, particularly with technologically sophisticated nations, to acquire resources, best practices, and standards. In an age of rapid scientific growth, this paper recommends reforms to create a judicial system that efficiently incorporates science and technology to ensure prompt and trustworthy justice.

Key words. Science , law , forensic ,artificial intelligence, cyber security

INTRODUCTION

The Relationship Between Science and Law

Scientific and legal paradigms are utterly differentiated from each other, yet are co-dependent disciplines that will continue to shape the world. Science offers methodologies that are adopted by the legal processes include forensic analysis, digital evidence authentication, and cyber forensic and others to make evidence to prove issues, to identify offenders and deliver justice. On the hand Law becomes the edifice of legislation that provides a frame work on which science operates within the ambit of the law to be both ethical and efficient in pursuit of justice.

Importance of Scientific Advancements in the Justice System

As the population grows and as technologies advance rapidly that the crime becomes more sophisticated, it is imperative to incorporate the science into justice system. Scientific methods help to manage evidence more effectively, investigate cybercrimes, and improve methods of identifying criminals for law enforcement and the judiciary[i]. High tech especially in forensic and digital sciences provides strong means of gathering, preserving, and analyzing evidence to enhance general fabric of all legal processes.

Purpose of the Study

This study aims to explore three main aspects: how science serves law, how in turn law helps the development of science, and technology shortcomings in Indian legislation. In this way, the study aims to stress the importance of the science as concerns enhancing Justice delivery, the regulatory place of law in scientific research, and ramifications of dint technologies in India justice systems.

Comparative Perspective

In order to compare India’s standing, this study will also describe the United States of America and other countries that effectively incorporated modern forensic and cyber technologies in the legal frameworks[ii]. This research makes it clear that India cannot afford to lag behind, and calls for the modernisation of the legal system, science and technology to enhance the justice delivery system.

SCIENCE AS A TOOL FOR LAW

Cybersecurity and Cyber Law

The rates of activity on the Internet have grown rapidly over the past few decades, so has the rate of cybercrime endangering people, companies, and states. Purdue offers reliable scientific tools to identify, analyze, and prevent cybercriminal activities, especially from the science of cyber security[iii]. Measures such as encoding, anti-malware scans, data loss control, and networks security standard procedures play a vital role in the security of bound digital

resources. Readily available are cutting-edge cybersecurity solutions including artificial-intelligence-based intrusion detection systems and harnessing the blockchain to secure transactions and verify their authenticity.

However, fighting cybercrime is still not easy. Malicious actions by cybercriminals are vast and diversified such as phishing, ransomware attack, hacking, and they are normally complex and hard to solve on an immediate basis. In India, it was observed that cases of cybercrime have risen dramatically in the recent past; for example, 52,974 cybercrime cases were reported in 2021[iv]. Washington through its Cybersecurity Information Sharing Act has developed cooperation structures between government and business organization making it more responsive to the threats than your typical corporate structure. This legislation permits the actual-time exchange of threat intelligence, which could possibly be replicated in India.

Forensic Science

A forensic science forms a unique partnership with law enforcement and the law. This partnership is unique because the members of each of these three fields know very little of the other two, but heavily depend on them. This is especially true regarding the lawyers knowledge of the forensic sciences. However, it is also true of the scientist understanding of the law[v]. Forensic science can help investigators to understand how blood spatter patterns occur (physics), learn the composition and source of evidence such as drugs and trace materials (chemistry) or determine the identity of an unknown suspect (biology). Its two peculiarities are that it is multi professional and multidisciplinary[vi].Of the later, fingerprinting is one of the most typical examples – it enables the authorities to provide an accurate match of the suspects to the scenes of the crime.

Toxicology which is the branch of science dealing with chemicals and poisonous substances has been useful in the analysis of cases of drug related crime and cases of poisoning. For instance, the Aarushi Talwar case in India completely depend upon the forensic evidence for analysing the details of crime scene[vii]. But, as highlighted in Part One, forensic infrastructure in India is still in its nascent stages. The United States has a better constitution of the forensic science that has large databases than the UK; for instance, it has CODIS (Combined DNA Index System) which leads to the quick and accurate matching of DNA[viii]. Labs with adequate funding, efficiently trained experts and such systems have gradually established forensic science as a far more reliable tool in justice system in the US than in India.

Digital Evidence and Expert Testimonies

Digital evidence collection and its authentication has now become critical in legal proceedings in cybercrime, fraud and violation of digital rights. Digital evidence involves information stored in computers, other electronic gadgets and in the network as well as in the transactions that occur through it. The actualization of digital evidence is required to prevent tampering of the data since it is very dynamic[ix]. To maintain evidence credibility hashing, data encryption, and chain of custody procedures are practiced. The use of experts is a vital part of litigation because such evidence is difficult to understand by the layman. Credentialed professionals contribute as witnesses who provide probative information to explain complex issues to trial adjudicators. In India there is a lack of specialized training for the judiciary as regards interpretation of scientific evidence and this results in occasional misjudgments. Although, the US law requires special orientation session on Scientific evidence for its judges and lawyers so that to enhance the reliability of the judicial system. Further, rules of evidence in United States entails the federal rules of evidence (FRE); that has influence in clearing doubts on admissibility of expert evidence.

Legislation Supporting Scientific Tools

Through statutes like the Information Technology (IT) Act, which deals with concerns like cybercrime, electronic signatures, and digital evidence, the Indian judicial system has made an effort to integrate scientific techniques and methodologies. However, there are several areas where the IT Act is vague, which makes it challenging to successfully prosecute some cybercrimes. Though there are still inadequacies, recent modifications have attempted to improve the IT Act. Given the lack of supplies and skilled personnel in Indian forensic labs, this investment is essential. Comprehensive laws such as the Electronic Communications Privacy Act (ECPA) in the US provide a strong legal foundation for the use of scientific instruments in the legal system[x]. The ECPA ensures that digital evidence is handled securely and legally by regulating the gathering, archiving, and admissibility of electronic communications in court. Even though it is changing, the Indian legal system still needs major improvements in infrastructure, scientific instruments, and laws to be on par with international norms.

HOW LAW SUPPORTS SCIENCE

Legal Framework for Scientific Research and Development

Legal regimes, notably Intellectual Property Rights, foster innovation by giving the proprietor exclusive ownership over the invention for scientific progress. Since rewards are provided for any invention in India, inventors have a legal right for 20 years to monopolize on their inventions and in the process, invention is continually done[xi]. India has witnessed considerable growth in patents and the grants of patents was from 9847 of 2016-17 to 28391 of 2021-22[xii].

These protections also prevent valuable investments and promote innovation, something especially true of industries, such as biotechnology and pharmaceuticals.

Most of the scientific studies are funded either by government or private organizations and institutions. DST and ICMR are major funding agencies of India offering grants to researchers Indian Department of Science and Technology (DST) and Indian Council of Medical Research (ICMR). For instance, the DST in the financial year 2020-21 had budgeted INR 6,000 crore for science and technology activities[xiii]. Furthermore, there are legal incentives, which include tax exemptions for R & D expenses to lure private companies to fund research for creating novel IT solutions or clean energy.

Privacy Laws and Ethical Boundaries

Standard procedures appear to be important enabling legislation in ethical scientific investigation, especially in areas where the privacy of individuals is of significant importance. Personal Data protection bill 2019 in India is another set of rules governing uses of data like the GDPR in the European Union[xiv]. If passed, this bill will include limitations on the gathering, storage, and utilization of data to safeguard personal data information while accommodating researchers who'll have limited access to the info. The National Bioethics Committee of the Indian Ministry of Health and Family Welfare regulates human subject participation in clinical trials, including informed consent and participant safety[xv]. This promotes public trust and responsible research.

International Cooperation and Legal Support

Global legal networking is important since it creates legal frameworks through which countries across the world may cooperate in scientific research. Some of the regional and bilateral agreements of this type are the Indo-US Science and Technology Forum (IUSSTF) that offers cooperation in research and development having subjects including renewable energy, health, space among others. The IUSSTF has facilitated in excess of 15000 exchange visits and more than 300 cooperative projects resulting in improved collaborative capacities of Indian and US researchers[xvi]. These partnerships enable the researchers to access ITC and resources from the other country and consequently giving both nations an improvement.

There are treaties like the Patent Cooperation Treaty under the WTO through which inventors can apply for the patents in various countries through a single application promoting international inventions. India became a member of the PCT in 1998 that enabled Indian inventors to protect their inventions abroad[xvii]. The trade related aspects of intellectual property rights agreement under the World Trade Organization aids in establishing the standards of the law in each member country whereby patent owners have rights in foreign markets. These international agreements mean that the countries can perhaps work together in matters that affect the whole world for instance global warming, diseases and space research. For instance, India's Mars Orbiter Mission (MOM) could draw on technical collaboration and information exchange with the US, although the possibilities of science cooperation were apparent[xviii].

CHALLENGES IN THE INDIAN ADMINISTRATION OF JUSTICE DUE TO LACK OF SCIENTIFIC TECHNOLOGY

Limited Forensic Infrastructure

The inadequacy of laboratory facilities and personnel remain major challenges to forensic development in India. Most of the state-owned forensic laboratories have inadequate equipment for DNA profiling, toxicology and digital analysis which are critical in cracking complex crimes. On the other hand, the United States has evolved a comprehensive Forensic system which include federal and state of the art forensic laboratories. For example, the crime lab of the FBI is a world reference in terms of forensic technology where they use complex techniques for DNA sequencing, ballistic and digital. The U.S. has also committed a lot of cash on databases such as CODIS and NIBIN, which assist in the sharing of information on bullets and ballistic more so in different states[xix]. They make it possible for the U.S to use forensic science as a tool for criminal investigation in a reliable real time integration level, which India is yet to achieve.

Digital Evidence Challenges

It turns out that e-evidencing poses several unique issues in India, primarily due in part to the lack of procedural regulation on how the digital evidence is collected, preserved, and authenticated. In this case, there is variability in how digital evidence presents itself in a court, and therefore its admissibility and reliability in trials gets impacted on. Furthermore, the United States states have more streamlined rules on use of digital evidence through the Federal Rules of Evidence (FRE) and the Electronic Communications Privacy Act (ECPA). The FRE lays down very rigorous standards of the admissibility, preservation and handling of digitally forged evidence such as hashing, time stamping and the creating of the chain of custody[xx]. This helps the US courts gain certainty and guarantee the integrity of technology-evidenced data that had not been altered and is acceptable to be presented in the court. Moreover, the U.S. has created such rules of law that could give more comprehensive legal solution for the problem of data privacy and digital surveillance, which would provide a stronger legal framework in handling the matters in the context of judicial proceedings on the use of electronic evidence.

Cybercrime Investigations

Nowadays, crime in the computer system has increased in India, but the actual and legal protection is not enough to fight it. The IT Act lies as the core Indian legislation against cybercrime and incorporates wrongs like hacking, cheating, identity theft and financial fraud. Nonetheless, it does not have contingency measures of the modern cybercrimes like ransom ware and artificial intelligence-facilitated cyber threats. The United States in particular has a rather more developed legislation to combat cybercrime investigation. Therefore, the United States enables the flow of threat intelligence between government and private sectors by way of CISA and the management of cybercrimes under the CFAA. The Department of Homeland Security and the Federal Bureau of Investigation are at the heart of managing national cybersecurity and are cooperatively involved with both global organizations and numerous technological corporations to ensure that they are always up to date[xxi]. This enables the U.S to work more efficiently on combating cyber criminals hence positioning it above in combating cyber threats – a factor India is in the process of developing in their system.

Delay in Judicial Processes

In the Indian context, the delay in case disposal is caused by manual intervention regarding evidence and lack of properly integrated systems within courts. Because of the lack of a centralized digital case management system, evidence is passed through a manual process, which results in the creation of additional time-consuming steps in the case-processing process. The problem also arises from the fact that investigative systems across the country are not well interlinked judicial systems thus dragging the clock faster for the delivery of justice in India.

The U.S., however, has embraced the use of electronic case management systems like PACER which offers access to electronic records, submission of electronic evidence, sharing of documents and real time follow up on completed cases[xxii]. This system grants convenient availability of case files in the courts of the federal system, which helps close cases much quicker with adequate transparency. The U.S. model shows how different stages of digital processing of cases and management of cases are helpful in increasing judicial effectiveness, a concept that India has started but not adopted entirely.

Expert Testimonies and Scientific Literacy in Court

The employment of expert opinions is regarded as fundamental to applying scientific findings in legal cases while some difficulties exist in the Indian courts. Many of the judges and lawyers have no academic background in the sciences, thus when faced with complexities in the expert's evidence, they end up either misunderstanding the evidence given or misinterpreting it. As the last line of evidentiary proof, the failure to provide check and balance on the methods used to select experts and assess their reliability throws the value of science into a precarious position within trials[xxiii]. The United States of America has embraced and applied the Daubert Standard which is very strict test that is used to determine the admissibility of the expert's evidence. This standard requires information introduced in court to have been developed by properly researched scientific methods and published research work. Also, the current training is still offered to the U.S. judges so that they can be in a position to understand and explain forensic and/or scientific information to the justice. In the United States, the approach is structured that scientific professionalism is involved in judiciary. The adoption of expert testimonies makes the trial more accurate and less biased.

COMPARATIVE STUDY: INDIA VS. THE UNITED STATES AND OTHER LEGAL SYSTEMS

Cybercrime and Cybersecurity

The major source of Indian law for cybercrime is the Information Technology (IT) Act, 2000 which prescribes different offenses like hacking, impersonation, cheating etc[xxiv]. Despite the IT Act has enacted from time to time, there are no specific provisions for dealing with the new form of cybercrime such as AI cybercrime and ransomware. However, many a time, the Indian law enforcement sectors face constraints related to infrastructure that hampers the procurement of evidence and cybersecurity measures. On the other hand, the United States has enacted different laws to counter every type of cyber threat. The Cybersecurity Information Sharing Act (CISA) authorizes the Department of Homeland Security to cooperate with the leaders of other federal entities and industry organizations in the sharing of cyber threat information to support quicker identification and addressing of cybercrime threats. Also, American organizations including the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI) and many others use modern cyberspaces to investigate cyber threats[xxv]. Such a framework ensures that cybercrimes are (radically) dealt with in the shortest time possible through support, resources and cooperation between various agencies, something that is still lacking in India's legal and cyber architecture.

Forensic Science in Legal Proceedings

The forensic system in India is relatively very weak, and most of the forensic laboratories have such problems as shortage of appropriate equipment and shortage of skilled professional. This means that forensic evidence used in the courts of India is always prone to delay and reliability issues. For instance, forensic DNA, fingerprints, and toxicology are available in a few official industry laboratories meaning that several high-profile criminal investigations get bogged down. Federal and state forensic centers employ the most modern methodological approaches which include fast DNA typing techniques and superior toxicological tests for criminal investigation purposes[xxvi]. The effectiveness of the U.S

forensic system is desirable by example of the FBI laboratory that runs codis, a national DNA database that quickens the identification of the suspect across states. This technological advancement relieves the circumstances of investigators from U.S. and helps them to solve various cases in better and more effective way.

Digital Evidence Regulations

Currently, the laws regarding the handling of digital evidence in India run under the IT Act that afford basic rules for the admissibility of electronic records. However, the chaotic, or rather loosely framed procedural protocols for gathering, preserving and most notably proving the admissibility of digital evidence have resulted in dissimilarities in treatments of cases. One of the difficulties that Indian courts encounter is the inability to provide proper authentication of digital evidence since proper norms for data control and examination, as well as the chain of custody of the evidence, is not guaranteed all over the world. The FRE provides rules including hash, time-stamp and encrypts to forestall tampering and this improves the admissibility of digital evidence. This degree of procedural form makes digital evidence to be more reliable and consistent in the courts of the United States. Similar guidelines should be prepared for the Indian judiciary to bring homogeneity in handling the digital evidence that in turn fortify the electronic records in trials.

Scientific Expertise in Courts

India has raised some problems in implementing scientific knowledge in its courts because there are no strict guidelines regarding experts' opinions. Evidence examiners, especially forensic and digital investigations, are often unappreciated or misunderstood by judges and juries as they are not usually trained in scientific knowledge or information. Even though Indian laws allow the presentation of experts over their respective fields there is very little direction on how these experts are chosen and assessed whose reliability influences the potency of scientific evidence presented[xxvii]. The United States responds to these difficulties by applying the Daubert Standard, an exacting criterion to determine the motion of an expert testimony. In its current form, these standard demands that scientific data submitted to court is conducted using valid methods and published studies. Also, the U.S. judges receive mandatory continuing education concerning scientific methods and forensic evidence, which prepare them to better comprehend the advanced analysis of evidence.

CHALLENGES AND RECOMMENDATIONS FOR IMPROVEMENT IN INDIA

Strategic forensic and cyber infrastructure improvements could aid India's legal system. Expanding forensic labs and creating specialised training centres would improve evidence processing by addressing resource and skill shortages. Investing in cyber labs and digital forensics will also help the country manage complicated cybercrimes. Judicial and law enforcement professionals need digital evidence, forensic science, and cybersecurity training. Specialised training would teach staff how to manage technical evidence for appropriate court interpretations and applications[xxviii]. Modernising evidence admissibility criteria need rules for handling digital and forensic evidence to ensure believability. Clearer expert testimony frameworks would improve trial scientific inputs. International ties with the US could supply superior technology and training. Participation in international treaties like the Budapest Convention on Cybercrime would strengthen cross-border collaboration and help India address cyber and forensic issues. These innovations would help the Indian legal system provide fast, technology-aligned justice.

CONCLUSION

Scientific advances improve justice delivery and legal frameworks guide responsible innovation. Due to poor forensic infrastructure, inconsistent digital evidence rules, and inadequate cybersecurity, India's court system struggles to use scientific technology. These gaps slow justice, taint evidence, and hinder criminal investigations and trials. Scientific advances are needed to solve these problems. A stronger legal system requires improving forensic and cyber infrastructure, modernising digital and forensic evidence admissibility laws, and educating judicial and law enforcement officers. International collaboration, especially with technologically advanced nations like the U.S., would provide India's legal landscape with insights, resources, and norms. India might improve its cyber and forensic science capabilities by attending foreign conventions and training programs. India can establish a modern, technologically adaptable justice system through reform and international partnership. These adjustments are necessary for quick, effective, and reliable justice delivery in an age of rapid scientific progress.

[1] Baranenko, D., Koval, A., Dulskyi, O., Lisitsyna, Y. and Musayev, E., 2023. Methodological principles of research in the field of ensuring evidence collection (on the example of cybercrimes): criminal-legal, criminal-procedural, and forensic aspects. *Amazonia Investiga*, *12*(67), pp.232-240.

[2] Dey, R., 2021. Law of Forensic Evidence in India and Abroad: A Comparative Study. *Issue 2 Int'l JL Mgmt. & Human.*, *4*, p.2879.

[3] Ahsan, M., Nygard, K.E., Gomes, R., Chowdhury, M.M., Rifat, N. and Connolly, J.F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, 2(3), pp.527–555. doi: https://doi.org/10.3390/jcp2030027.

[4] Bharath Kancharla (2023). *Data: In 20 Years Between 2002 & 2021, Five States Accounted for More Than 2/3rd of the Cybercrimes Reported in India*. [online] FACTLY. Available at: https://factly.in/data-in-20-years-between-2002-2021-five-states-accounted-for-more-than-2-3rd-of-the-cybercrimes-reported-in-india/

[5] Richard Saferstein, Forensic Science Handbook 2 (New Jersey State Police, Prentice Hall Regents 2015).

[6] Bapuly –Forensic Science – IT'S Application in criminal investigation 1(Paras Medical Publisher 2006).

[7] Mandhani, A. (2023). *Lack of funding, underequipped labs — a study by NLU's Project 39A finds gaps in Indian forensics*. [online] ThePrint. Available at: https://theprint.in/judiciary/lack-of-funding-underequipped-labs-national-law-university-study-finds-gaps-in-indian-forensics/1747846/.

[8] [viii] Wickenheiser, R.A., 2022. Expanding DNA database effectiveness. *Forensic Science International: Synergy*, *4*, p.100226.

[9] Kiener-Manu, K. (2019). *Cybercrime Module 6 Key Issues: Handling of Digital Evidence*. [online] www.unodc.org. Available at: https://www.unodc.org/e4j/zh/cybercrime/module-6/key-issues/handling-of-digital-evidence.html.

[10] Bureau of Justice Assistance (1986). *Electronic Communications Privacy Act of 1986 (ECPA)*. [online] Bureau of Justice Assistance. Available at: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285.

[11] Khan, B.Z., 2020. *Inventing ideas: patents, prizes, and the knowledge economy*. Oxford University Press, USA.

[12] Ahaskar, A. (2022). *Patents granted in India tripled in last 5 years; still a fraction of China, US*. [online] mint. Available at: https://www.livemint.com/companies/start-ups/patents-granted-in-india-tripled-in-last-5-years-still-a-fraction-of-china-us-11643630387938.html

[13] Ministry of Science & Technology (2020). *Annual Report*. [online] Department of Science and Technologies . Available at: https://dst.gov.in/sites/default/files/Annual%20Report%202020-21%20in%20English.pdf.

[14] Prasad M, D. and Menon C, S., 2020. The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology*, *28*(1), pp.1-19.

[15] Selvarajan, S., Behera, S., Das, S., Xavier, A. and Anandabaskar, N. (2019). Indian Council of Medical Research's National Ethical Guidelines for biomedical and health research involving human participants: The way forward from 2006 to 2017. *Perspectives in Clinical Research*, 10(3), p.108. doi: https://doi.org/10.4103/picr.picr_10_18.

[16] Thornley, P., Rathi, B., Borah, A.J., Saha, B., Adams, J., Hiloidhari, M., Blanchard, R., Dinsdale, R., Nagarajan, S., Kumar, S. and Vaidyanathan, S., 2022. Bioenergy Technologies for a Net Zero Transition: outcomes of UK-India Bioenergy research scoping.

[17] Jawale, K.V., 2023. *Indian Intellectual Property Rights*. Academic Guru Publishing House.

[18] Goswami, N. and Garretson, P.A., 2022. The Rising Salience of "NewSpace" in India: Prospects for US-India Space Cooperation. *New Space*, *10*(1), pp.87-100.

[19] ATF (2019). *National Integrated Ballistic Information Network (NIBIN) | Bureau of Alcohol, Tobacco, Firearms and Explosives*. [online] Atf.gov. Available at: https://www.atf.gov/firearms/national-integrated-ballistic-information-network-nibin.

[20] Vedwal, A., 2023. Admissibility of Digital Evidence for Cyber Crime Investigation. *Available at SSRN 4443356*.

[21] Department of Homeland Security (2022). *Cybersecurity*. [online] www.dhs.gov. Available at: https://www.dhs.gov/topics/cybersecurity.

[22] Chawinga, W.D., Chawinga, C., Kapondera, S.K., Chipeta, G.T., Majawa, F. and Nyasulu, C., 2020. Towards e-judicial services in Malawi: Implications for justice delivery. *The electronic journal of information systems in developing countries*, *86*(2), p.e12121.

[23] Canela, C., Buadze, A., Dube, A., Jackowski, C., Pude, I., Nellen, R., Signorini, P. and Liebrenz, M. (2019). How Do Legal Experts Cope With Medical Reports and Forensic Evidence? The Experiences, Perceptions, and Narratives of Swiss Judges and Other Legal Experts. *Frontiers in Psychiatry*, 10. doi: https://doi.org/10.3389/fpsyt.2019.00018.

[24] Chander, H. and KAUR, G., 2022. *Cyber laws and IT protection*. PHI Learning Pvt. Ltd..

[25] FBI (2016). *National cyber investigative joint task force | federal bureau of investigation*. [online] Federal Bureau of Investigation. Available at: https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

[26] Gardner, E.A., DellaRocco, R. and Bever, R., 2022. Forensic Science in the United States. I: Historical Development and the Forensic Science Laboratory System. *Forensic Science Review*, *34*(2), pp.72-82.

[27] Dhingra, A. (2019). *Expert witnesses under the Indian Evidence Act, 1872*. [online] iPleaders. Available at: https://blog.ipleaders.in/expert-witnesses-under-the-indian-evidence-act-1872/.

[28] Schwarcz, D., Wolff, J. and Woods, D.W., 2022. How privilege undermines cybersecurity. *Harv. JL & Tech.*, *36*, p.421.