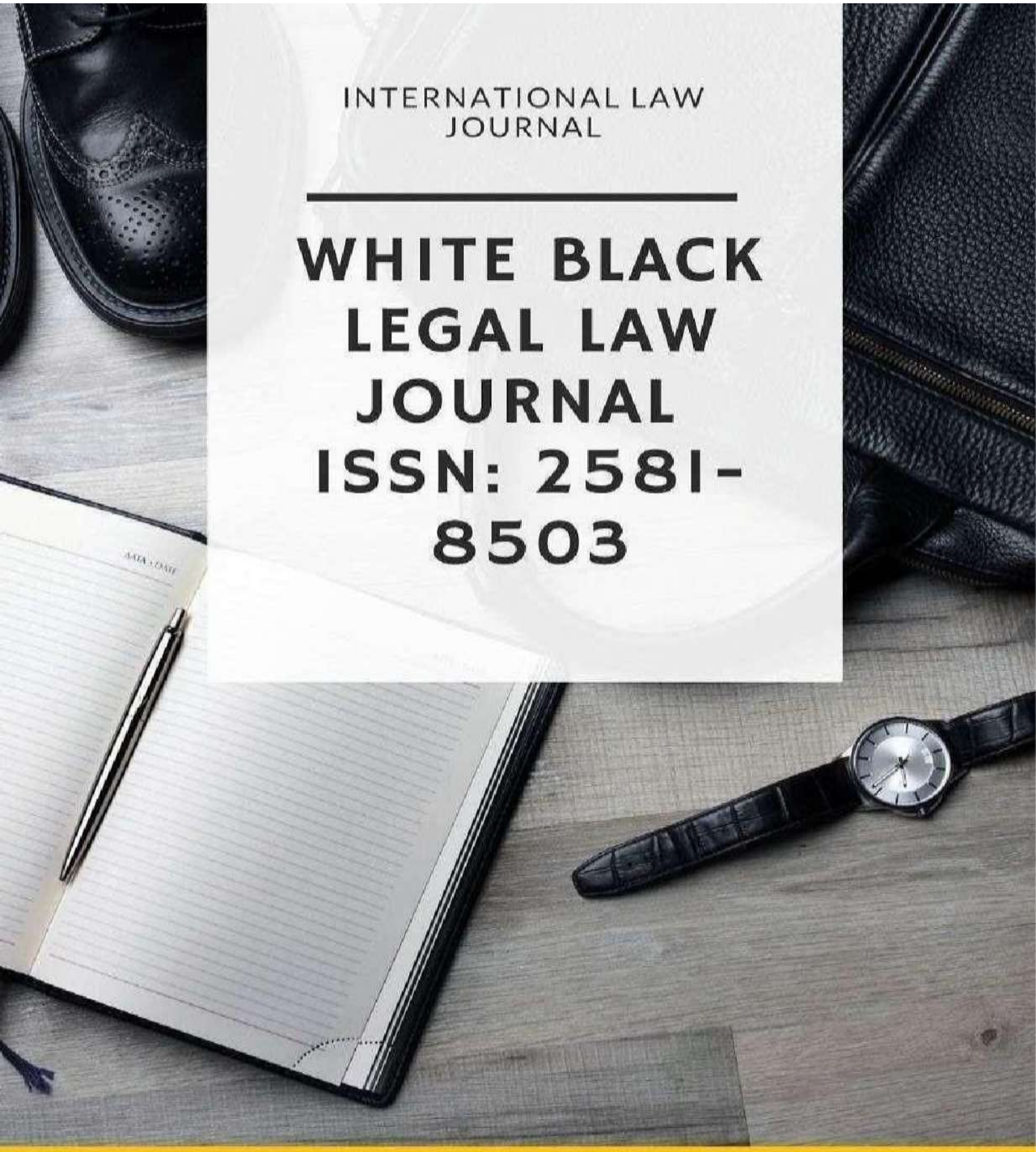

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

LEGAL IMPLICATIONS OF DIGITAL FORENSIC EVIDENCE

AUTHORED BY - SARTHAK DHOUNDIYAL

When conducting an investigation, an investigator is required to adhere to stricter ethical standards. Participants in digital forensics investigations should be treated fairly, equally, with respect. Ethical consideration is essential when performing digital forensics investigations. Every individual involved in a digital forensics investigation ought to maintain the utmost impartiality. Digital forensics ethics are necessary for a comprehensive efficient investigative process. Our ultimate objective is to deeply comprehend digital forensic ethics within you. Stay tuned for more information.

Cyber Ethics

"Digital ethics" is the branch of ethics that studies the collection of laws moral principles that control how people behave with one another in marketplaces, organizations, society at large when computers are used as a medium. This code of ethics for digital activity aims to establish standards of behavior that nonprofits should adhere to when engaging in digital activities, such as using social media to reach a larger audience using donor data to guide fundraising campaigns. How Ethics in Digital Forensics Operate

Evidence retrieved from digital forensics investigations may be compromised. It is your responsibility to conduct in-depth research, to speak the truth, to remain impartial. Your personal professional values define your baseline conduct.

Investigative success in Digital Forensics requires adherence to a certain set of ethical guidelines that practitioners must follow. This means protecting discretion, avoiding conflicts of interest, ensuring that their actions follow the law moral standards.

Analysts in digital forensics must remain impartial objective throughout the investigation. It is essential that they stay clear of any bias or biases that could affect how they look at understand the evidence.

In certain circumstances, obtaining permission to gather examine digital evidence may be necessary. This is especially true in circumstances where people have a right to privacy, including while using personal technology or communicating.

Digital forensic investigators must abide by all applicable rules regulations, including those relating to intellectual property, data privacy, data protection. To stay current with the newest methods resources, digital forensic investigators should seek out chances for continuous learning development.

Legal Concerns in Digital Forensics Inquiries

The digital forensics procedure must adhere to legal criteria in order to guarantee that the data collected is appropriate in court does not violate any laws. Here are some legal issues that digital forensics may face.

The US Constitution's Fourth Amendment forbids arbitrary searches seizures. Before conducting a search or seizure, digital forensic investigators must adhere to legal procedures, get a warrant, or have other valid justifications.

The chain of custody documents the evidence's acquisition transportation before it is presented in court. Digital forensic investigators have strict requirements to adhere to in order to maintain the evidence's integrity, admissibility, chain of custody.

All admissibility requirements set forth by law, such as dependability, authenticity, relevance, must be met by digital evidence. Digital forensic investigators must adhere to standards procedures to make sure the data they gather satisfies legal criteria.

Digital forensic investigators are required to follow all applicable laws pertaining to data protection privacy. Investigators are obligated to respect the privacy of personal data exercise caution when accessing or disclosing any data that is not necessary for their work.

Digital forensics investigations can take place across multiple jurisdictions, investigators must follow local laws wherever they operate. Jurisdictional issues can complicate digital forensics investigations, therefore investigators must be aware of the rules that apply to the data they collect.

Analyzing intellectual property, such as trade secrets, copyrighted content, other items, may be

part of digital forensic investigations. To avoid violating any copyright or other intellectual property rights, investigators must adhere to all applicable intellectual property laws.

Digital forensics investigations must take legal considerations into account to ensure that the evidence collected is reliable for use in court does not violate any laws. Digital forensic investigators need to be aware of legal issues pertaining to jurisdiction, search seizure, chain of custody, admissibility of evidence, data privacy protection, intellectual property.

The Computer Forensic Analysis Process

Data collection is typically the initial stage in a computer forensic examination approach. Computer experts ensure data integrity by retrieving data from digital devices using certain techniques tools.

Following acquisition, data preservation becomes crucial. This is a crucial step since it prevents data loss or manipulation. Additionally, it prepares data for inspection, during which forensic computer experts review data search for digital evidence that may be relevant to the case. This stage usually necessitates the use of advanced software analytical methods in order to fully utilize the potential power of digital evidence.

The last step in the procedure is reporting. This means providing analysis results to legal specialists. Expert testimony must be admitted under the Daubert standard, which requires that the results be presented in an intelligible clear manner. This can affect how the defense presents its case ensures that decisions made in court will be upheld.

Case law:

Admissibility of digital evidence

For digital evidence to be admissible in a court of law, a number of legal technical conditions must be satisfied (Antwi-Boasiako, Venter, 2017). In relation to the former, the court considers the legitimacy of searches seizures of data, communication technology, associated information, as well as the applicability, authenticity, integrity, dependability of digital evidence (Antwi-Boasiako, Venter, 2017). Concerning the latter, the court scrutinizes digital forensics practices,

instruments for extracting, preserving, analyzing digital evidence, digital laboratories for conducting analyses, reports from digital forensic analysts, the academic technical credentials of these analysts as well as expert witnesses (if needed) (Antwi-Boasiako, Venter, 2017). The Harmonized Model for Digital Evidence Admissibility Assessment (HM-DEAA), a framework created by Antwi-Boasiako Venter (2017), summarizes the fundamental legal technical elements that determine the admissibility of evidence. In specifically, the HM-DEAA proposes a three-phase method for evaluating digital evidence that includes assessment, consideration, determination of admissibility. The HM-DEAA framework is used in the section that follows to highlight the legal technological requirements that are frequently applied in different jurisdictions to ensure that digital evidence is admissible in national courts.

Evaluation of Digital Evidence

During this phase, courts evaluate whether the necessary legal power was obtained to conduct searches, obtain seizures, handle information communication technology (ICT) related data. Examples of legal authorization include a search warrant, subpoena, or court order. The legal prerequisites for acquiring ICT ICT-related data are determined by national laws in each jurisdiction (see to Cybercrime Module 7 on International Cooperation against Cybercrime). Nonetheless, the legal tool that countries most commonly use to seize ICT is search warrants. However, different national laws have varied requirements for legal orders based on the facts of the case, the circumstances surrounding the search seizure, the credentials of the people conducting the search. See Cybercrime Module 7 on International Cooperation against Cybercrime for further details on the legal orders required to access data within various jurisdictions.

The forensic relevance of digital evidence is also evaluated during this phase. Digital evidence is deemed relevant for forensic purposes if it can: establish or disprove a link between the offender the target (victim, digital device, website, etc.); corroborate or contradict the testimony of the offender, victim, and/or witnesses; identify the offender or perpetrators of cybercrime; provide leads for investigation; provide details about the offender's method of operation (modus operandi, or M.O.) (i.e., habits, techniques, distinctive features of their behavior); demonstrate the occurrence of the crime (corpus delicti) (Maras, 2014; Maras, Miranda, 2014).

Considering Digital Evidence

During this phase, the digital forensics protocols, tools used to gather evidence, credentials experience of experts who collected, stored, analyzed data (the credentials experience of experts vary by country; see Cybercrime Module 5 on Cybercrime Investigations), digital forensics labs where data was processed analyzed are all examined to assess the integrity of digital evidence (US National Institute of Justice; 2004a; Maras, 2014). This evaluation essentially aims to ascertain whether standards were met for handling examining digital evidence, whether scientific principles were applied to preserve, acquire, analyze it (e.g., whether digital forensics tools were validated, up-to-date, properly maintained, tested before their use, to ensure their proper functioning).

In court, digital forensics experts testify about their qualifications, the operation of digital devices, online platforms, other ICT-related sources, the digital forensics process, the rationale behind the use of a particular digital forensics tool over others, the preservation, acquisition, analysis of digital evidence, the interpretation of the results of these analyses, the accuracy of these interpretations, any potential alterations to data the reasons behind them (US National Institute of Justice; 2004a; Maras, 2014).

The credentials of experts in the field of digital forensics are also carefully examined in order to assess the competence of those managing evaluating digital evidence. This ability is required to ensure that work products meet quality standards that results are assured (SWGDE Overview of Accreditation Process for Digital Multimedia Forensic Labs, 2017). That being said, there are no standard qualifications for the proficiency of digital forensics practitioners. Each nation has different requirements for experts in digital forensics (UNODC, 2013). Depending on the country, accreditation of professionals in digital forensics may or may not be necessary (UNODC, 2013). As a result, this step determines if specialists are competent to provide expert witness testimony and/or carry out suitable analyses of ICT ICT-related data. It is also decided if the competences of these analysts specialists were verified assessed.