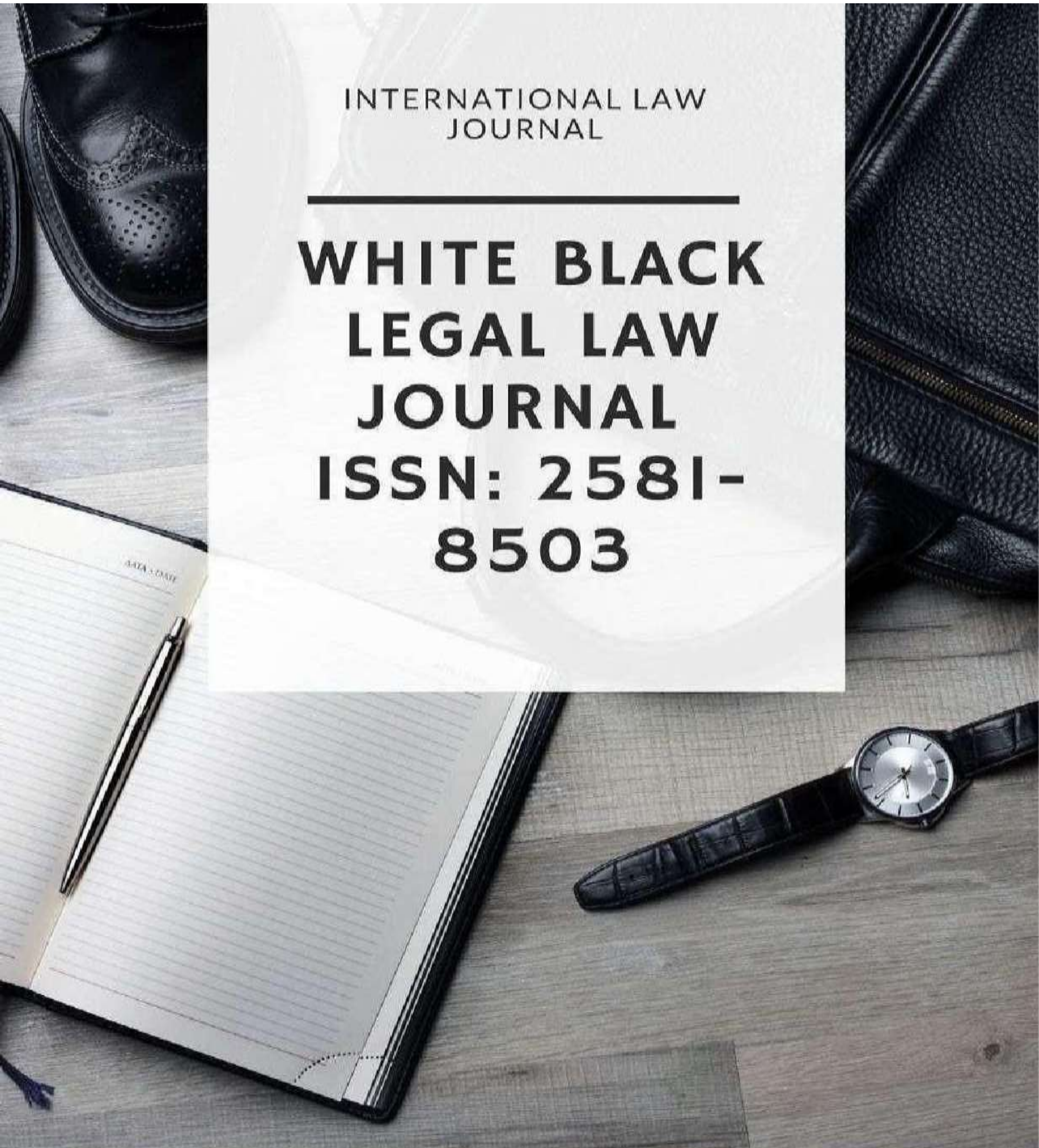


INTERNATIONAL LAW JOURNAL

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.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.

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

"NAVIGATING THE LEGAL LANDSCAPE: DIGITAL SIGNATURE FRAMEWORK AND REGULATORY CHALLENGES IN INDIA"

AUTHORED BY: A. MUKUNDH VISWESH

ABSTRACT

In today's digital world, digital signatures have become increasingly vital in maintaining electronic documents and transactions' validity, integrity, and security. Recognizing the importance of digital signatures, India has built a strong legal framework to oversee their use. This summary comprehensively overviews India's legislative framework governing digital signatures.

The Information Technology Act of 2000 and its revisions laid the groundwork for digital signatures in India. Digital signatures are legally recognized as authenticating electronic data and papers under this statute. The Controller of Certifying Authorities (CCA) was established as a regulatory entity responsible for licensing and regulating Certifying Authorities (CAs) that issue digital certificates to facilitate the usage of digital signatures.

CAs, which are authorities responsible for authenticating the identification of individuals or organizations wanting to receive a digital certificate, issue digital signatures in India. These certificates contain the holder's public key and are used to create and validate digital signatures. CAs' operational guidelines are outlined in the Information Technology (Certifying Authorities) Rules, 2000.

Adopting the Aadhaar-based e-KYC (Know Your Customer) process is one of the important breakthroughs in India's regulatory framework for digital signatures. Aadhaar, a one-of-a-kind biometric identity system, enables individuals to obtain digital signatures swiftly and easily, promoting their use in various applications, including government services.

Furthermore, the Indian government has taken steps to ensure digital signature security by requiring the adoption of cryptographic standards and digital signature algorithms in Digital Signature Certificates (DSCs). These standards are revised on a regular basis to keep up with technological advances and emerging dangers.

Finally, India's digital signature legal framework has evolved to meet the demands of the digital era, ensuring the legal validity and security of electronic transactions and documents. This framework, which is based on the Information Technology Act of 2000 and is supported by regulatoryorganizations such as the CCA, is critical inbuilding trust and confidence in digital interactions acrossmany industries in India. This study further covers other areas that come within the legal framework.

Introduction

The introduction of information technology completely changed the world, and gratefully, India took the lead and attracted attention from all around the world. The Information Technology Act 2000 (The Act), passed by India, was enacted on October 17, 2000. The Act applies to everyone in India, including those who commit crimes abroad. The Act establishes the validity of digital signatures and makes it possible for users to use them in the same way as traditional signatures. A digital signature serves the same fundamental function as a traditional signature. Therefore, the goals are to verify the document's authenticity, ascertain the signer's identity, and connect the document's contents to the individual providing a digital signature.

In his book Cyber Laws, Justice Yatindra Singh said that the hash function is employed to convert a message into a distinct, shorter fixed-length value known as the hash result since public key encryption is laborious and inefficient. The hash function serves as the original text's index. It is the mapping or translation of one sequence into another using an algorithm. The hash function is designed such that, when applied to the same electronic record, it yields the same hash result each time; two electronic records, however, cannot yield the same hash result when applied to the same hash function. Put differently, mapping is one-to-one rather than many-to-one. One way is this. The hash result cannot be used to recreate the original message. A digital signature is created by encrypting a message's hash result using the sender's private key.

DS identifies the sender and confirms the legitimacy of an electronic document. It makes the sender/filer's identity very evident. Such a signature can be used or regarded as equivalent to other signatures that have previously been accepted by law since the IT Act of 2000 gives it legal sanction. The United Nations Commission on International Trade Law's (UNCITRAL) Model Law on Electronic Commerce and early e-commerce enabling laws like the Utah Digital Signatures Act of 1995, the Singapore Electronic Transactions Act of 1998, and the Malaysian Electronic Signatures Actserved as the model for the Act.

The two distinct facets of the technology revolution are the subject matter of the Act. One is the provision of legal recognition to electronic transactions and the use of alternatives to paper-based methods of communication, storage, etc.; this is specifically mentioned in the Preamble of the Act.

The Act aims to identify a number of offences related to the use of digital signatures and establish regulations for them. It's interesting to note that, in contrast to the majority of previous laws of a similar nature, the Act also attempts to govern the Internet by making it illegal to publish offensive content online.

ELECTRONIC SIGNATURE AND DIGITAL SIGNATURE

Even though a lot of people use it interchangeably quite frequently. However, a more thorough examination reveals that the term "electronic signature" is extremely broad and that "digital signature" is merely one of the numerous types of electronic signatures that can be imagined.

Section 2(ta) of the Information Technology Act 2000 (as amended by the Information Technology Amendment Act 2008, or ITAA) defines an electronic signature as follows: Digital signatures are included in the definition of electronic signature, which is the subscriber's authentication of any electronic record using one of the electronic techniques listed in the second schedule. ***Section 2(p)*** defines the term "digital signature" as follows: A digital signature is an electronic record that has been verified by a subscriber using an electronic method or procedure in compliance with ***Section 3's*** requirements.

Digital Signature	Electronic signature
A digital signature relies on public key infrastructure which authenticates the electronicsignature	An electronic signature is simply a legally validelectronic replacement of a handwritten signature.
Digital signatures carry a user's information along with electronic signatures.	Electronic signatures do not contain any authentication attached to them.
A digital signature secures a document.	An electronic signature verifies the document.
Digital signatures are validated by licensed certifying authorities.	Electronic signatures are not validated by licensed certifying authorities.
Digital signatures come with encryption standards.	Electronic signatures do not come with encryption standards.
A digital signature consists of various security features and is less prone to tampering.	An electronic signature is less secure and is morevulnerable to tampering.
A digital signature acts as an electronic fingerprint that consists of a person's identification.	An electronic signature can be a file, image, or symbol attached to a document to give consentfor a signature.
A digital signature is created via cryptographicalgorithms.	An electronic signature offers lower security andno cryptographic algorithms are used in creatinga simple electronic signature.
A digital signature is authenticated using a digital signature certificate.	An electronic signature is authenticated using aphone number, SMS, etc.

Digital Signature Certificate (DSC)

Digital certificates function as a person's identification for certain purposes; for example, a driver's license identifies a person who is authorized to drive in a given nation. Similarly, you may electronically establish your identity or your authorization to access data or services on the Internet bypresenting a Digital Certificate. The electronic versions of physical or paper certificates, such as your passport, membership card, or driver's license, are called digital certificates.

Let's check the DSC's statutory definition. The definition of "Digital Signature Certificate" is given in ***Section 2(q)*** of the Act and is not expanded upon. It states that a Digital Signature Certificate• produced following Subsection (4) of Section 35 qualifies. The entities recognized as CAs (Certifying Authorities) are the ones who issue DSCs. The process by which the Certifying Authorities (CA) provide an electronic or digital signature is covered in ***Section 35. Section 35(4)*** states that the Certifying Authority may, upon receipt of an application under sub-section (1), grant the Digital Signature Certificate or, for reasons to be recorded in writing, reject the application after reviewing the certification practice statement or the other statement under sub-section (3) and conducting any necessary inquiries. However, no application shall be denied unless the applicant hasbeen given a reasonable opportunity to contest the proposed rejection.

In India, digital signature certifications are recognized by law. Digital signature certificates can be used, according to the Indian government's provisions under the Information and Technology Act, of 2000. Digital signature certificates can be used to sign documents that are provided electronically. TheCertifying Authorities (CAs) are authorized by the Controller of Certifying Authority (CCA) to issue certificates for digital signatures.

TYPES OF DIGITAL SIGNATURES

There are 4 different types of digital signature certificates in India.They are

1. Class 0 Certificates
2. Class 1 Certificates
3. Class 2 Certificates
4. Class 3 Certificates

Explanation

Class 0 Certificate: This certificate is solely intended to test the certificate and familiarize yourself with it. With the many applications across a range of domains where digital signature certificates are used.

Certificate of Class 1: Individuals or private subscribers can use this certificate. These certifications attest that in the database of the Certifying Authorities, a user's name or email address identifies them.

Class 2 qualification: This qualification is utilized by both private citizens and employees of businesses. These endorsements will verify that the data provided in the application by the subscriber does not contradict the information from reputable consumer databases

Class 3 qualification: Both people and organizations utilize this qualification. This high affirmation certificate is meant mainly for use in electronic commerce. Individuals can only receive this certificate upon making a personal appearance in front of the Certifying Authorities.

Laws governing Digital Signature in India

Digital Signature in India is governed by:

(A) Information Technology Act, 2000 (ITA):

All electronic signature operations are based on these e-signing laws. The Act of Information Technology 2000 (ITA) is the main legislation that governs e-signing in India. The ITA establishes fundamental guidelines for adhering to e-signature requirements.

(B) The Indian Contract Act 1872

It is controlled by the fundamental concepts of contracts, including offer and acceptance, free consent, capacity, and legitimate compensation, and it gets its legal standing from Section 10 of the Indian Contract Act, of 1872. Similar to this, with click wrap agreements, the terms and conditions are presented as an offer, which the user accepts by clicking "I Agree." According to ***Section 4*** of the Information Technology Act of 2000, information that is in electronic form and easily available for future reference is considered to satisfy any legal requirement of physical records that requires information to be in printed or typewritten form. Furthermore, ***Section 10(A)*** of the IT Act confers legitimacy by acknowledging the creation, acceptance, and revocation of contracts in digital format.

An electronic contract is saved or documented with the parties concerned in electronic form as an electronic record after it is executed. The fact that it is an electronic form does not make it unenforceable. The Chennai High Court has implemented and affirmed these clauses in the Tamil Nadu Organic v. State Bank of India xviii (2019) case. The results of the electronic auction were maintained, and the Court said that obligations might result from these kinds of electronic agreements and methods as long as the fundamental terms of the agreement are met and the Contract Act's legal provisions are followed. As a result, e-contracts are often enforceable in court and have legal standing.

(C) The Indian Evidence Act, 1872

To align with the IT Act's introduction of electronic document execution, the Indian Evidence Act, of 1872 was also modified. The Indian Evidence Act of 1872, ***Section 65A***, acknowledges the admission of electronic documents as evidence. It says that under the terms of ***Section 65B*** of the aforementioned Act, the contents of electronic recordings may be proven. In addition to allowing for the acceptance of electronic evidence, ***Section 65B*** of the Indian Evidence Act, of 1872 stipulates thatany information stored in an electronic mode that can be printed on paper, stored, recorded, or copiedin optical or magnetic media created by a computer is considered a document and is admissible in anyproceedings without the need for additional proof or the production of the original as evidence or any of its contents. A certificate certifying the electronic record containing the statement and outlining its presentation format must be supplied, according to ***section 65B(4)***, in addition to the previously mentioned requirements. According ***to Section 73A*** of the Evidence Act, 1872, a person, the Controller, the Certifying Authority, or any other person may be ordered by the Court to use the public key specified in the Digital Signature Certificate to validate the digital signature that has been purportedly affixed by that person in order to determine whether it is indeed theirs. According to ***Section 47A*** of the Evidence Act of 1872, the view of the certifying authority that issued the electronic signature certificate is a significant fact when the Court is asked to express its opinion about an individual's electronic signature. According to ***Section 85B*** of the Evidence Act, of 1872, thecourt will assume, absent proof to the contrary, that

a) the secure electronic record has not been modified from the particular moment the secure status corresponds to;
b) The subscriber attaches the secure digital signature to endorse or endorse the electronic record.

According to **Section 85C** of the Indian Evidence **Act of 1872**, the court would assume that a document is authentic and accurate if a digital signature is attached to it.

(D) The Companies Act, 2013

Over the course of the last 152 years, India has operated under the Indian Penal Code (IPC) withgreat success. In light of information technology development, It was deemed that further measures were required to handle the latest advancements in the information technology and electronics fields. Consequently, using information technology The 2008 IPC Amendment Actwas also modified. The identical clause as in has been included as ***Section 73A***. The Indian Evidence Act, ***section 47A***. Additionally, Section 464 has been changed to state that the aforementioned section should be extended to electronic signatures and electronic documents aswell. When a person is accused of creating a fake paper or electronic record, ***Section 464*** addresses those circumstances. Forging of electronic records is likewise permitted by ***Section 466.Sections 4, 40, 118, and 119*** of the IPC have been amended.

(E) Certifying Authority

The Act gives CAs access to a licensing system that recognizes foreign certificates[1]. The Controller of Certification Authorities ("Controller"), who is tasked with licensing, certifying, supervising, and monitoring the operations of CAs, is principally responsible for regulating CAs[2]. The Controller's duties encompass the whole range of tasks, such as:

- The standards to be maintained,
- The qualifications and experience of employees of CAs,
- The form and content in which accounts shall be maintained by CAs,
- The form and content of a digital signature certificate and the key, and,
- Resolving any conflict of interest between the CAs and the subscribers.

Furthermore, on October 17, 2000, the Central Government[3] published the Certifying Authority Rules ("CA Rules"), which outline the requirements that must be met in order for CAs to operate and submit an application for a license in India. The CA Rules contain within their purview, provisions as regards various aspects such as:

- Composition of applicant company or partnership firm;

[1] Chapters VI, VII, and VIII of the Act.

[2] Sections 17 and 18

[3] In exercise of its powers under Section 87(2) of the Act

- Networth requirements;
- PKI technology to be used for digital signatures;
- Certificate Standard;
- Location of facilities;
- Cross-certification standards
- Database standards;
- Period of license, subscriber's private key, subscriber’s public key, CA private key, CA public key; and,
- Process of generation, issue, verification, archival, etc of DSCs.

ISSUES AND USE OF DIGITAL SIGNATURE

(A) Technology

As was previously indicated, the Act has established extremely precise standards for the technology that must be employed in authentication systems. According to Section 3 of the Act, "the electronic record's authentication shall be carried out by the use of the hash function and asymmetric cryptosystem.

Moreover, the CA Rules' Rules 6 and 7 specify specific technological requirements that must be adopted concerning the digital signatures that Indian legislation will allow to be provided.
Insidethe Under the Act's framework, the Rules stipulate that all DSCs must adhere to the specified standard.

These regulations are comparable to those found in Malaysian and Singaporean laws, both of which have centered their e-commerce development upon public key infrastructure.

However, the United States of America's governmental Electronic Signatures in Global and National Commerce Act is technology-neutral, supporting any method that can logically link an individual with an electronic record.

As was previously indicated, authentication techniques are provided by several various technologies. New technologies would be validated by a technology-neutral provision based on the tenet that they should be able to rationally and consistently link a communication to a specific person.

Stronger and more trustworthy authentication methods would not be accepted as producing digital signatures that are legitimate under the Act under the current Indian framework.

(B) Identification

Following ***Section 36(e)***, the CA must depict the data in the DSC as correct when issuing it. Per Rule 10, the data in the Certificate comprises the subscriber's name whose public key is recognized by the specific DSC.

Moreover, the CA must adhere to the process outlined in the CPS per Rules 25(2) to confirm identity (i.e., using the "subscriber identity verification method" described under Rule 2(k) as a technique for confirming and authenticating a subscriber's identification). The approval of this subscriber identity verification technique would need to come from Operator[4].

In relation to these verification processes, neither the Act nor the CA Rules provide instructions or guidelines with respect to the procedure. The Controller would presumably have the last say in selecting the techniques used by the CA, as the subscriber verification method would be subject to Controller oversight. The CA may still be accountable for ensuring that the subscriber's identity is verified and authenticated even if the Controller grants consent.

Regarding the possibility of outsourcing certain identification processes, neither the Act nor the CA Rules make any explicit mention of it. This kind of outsourcing to a designated registration authority doesn't seem to be prohibited. However, as the CA would be held accountable for the registration authorities' acts, they would likely be viewed as trustworthy individuals.

(C) Types Of Certificates

A digital signature is defined by the Act as one that verifies a subscriber's production of an electronic

[4] As provided under Rules 10(ii)(b) & 23(e)

record[5]. Furthermore, any individual in whose name the DSC is issued is defined as a subscriber under ***Section 2(zg).***

The Act's Chapters VI, VII, and VIII lay forth the parameters for the interaction between both the CA and the subscriber. The principal duties of the CA with respect to subscribers are as required by the Act. These are the minimal requirements that a CA must meet time it sends out a DSC.

Around the world, the digital signature market often provides several types of signatures based on individual subscribers. A certificate's classes are distinguished from one another by a variety of factors, including (a) security level, (b) cost, (c) validity time, and (d) limitations on the use of DSC.

According to ***Section 10*** of the Act, the Central Government can establish regulations on digital signatures, including "the types of digital signatures". Additionally, a notion of "secure digital signatures" as opposed to regular digital signatures is proposed in ***Section 15***. As was previously stated, the implementation of a security protocol "agreed between the parties concerned" is the foundation for the "secure" status. Although certain interpretations of the Act's provisions and the Rules[6] appear to indicate that subscribers to any DSCs under the Act have the same rights and obligations, there is a considerable question regarding the distinction made by ***Section 15*** in favour ofsecure digital signatures.

Distinctions based on security level and DCS use limitations would not be feasible under the current circumstances. As was previously established, to issue a DSC, a CA must adhere to specific minimum security requirements as required by the Act. A DSC would not be recognized if its level was lower than the minimal requirements. Furthermore, under the Act, there is no benefit to using a digital signature with higher security standards than necessary in place of a physical signature[7]. As a result, itmight not be immediately apparent to a customer what the legal standing of a digital signature offers.

[5] Section 2(p)

[6] Sections 3, 5, 15, 30, 35 and 36 amongst other provisions

[7] The only exception to this is the favourable presumption under Section 15.

(D) Group Certificates

The provision of DSCs to corporations or groups of individuals also presents another issue. concerns inside the Act's structure. The person in whose name the DSC is issued is defined as a "subscriber" under ***Section 2(zg).***

Rule 2(i) states that a "person" can be an individual, a firm, an association, or a group of persons, whether or not they are incorporated. It can also refer to the federal government, a state government, or any of its ministries, departments, agencies, or authorities. Consequently, it appears that the Act intends to allow DSCs to be issued to groups of people or legal entities such as corporations. It is equivalent, then, to fuse in the real world the Company seal with the authorized representative's signature without disclosing who the authorized person was. The Act is ambiguous, therefore, about how these corporations' or groups' identities and actions would relate to their legal standing and ability under other current laws.

When a juristic person receives a DSC, the decision on who would be the "Named Entity" and who the "subscriber" is difficult, to say the least. The relationship between the Subscriber and the Named Entity gets quite intricate. This entails defining the circumstances under which a person may act on behalf of a juristic person. This is subject to several other laws as well as the guidelines established bythe legal individual An entity that does not have the legal standing or the power to enter into contracts under the currentlaws may be able to receive identification under the Act, along with the authority to authenticate documents. Therefore, even if a DSC is legitimately granted to such an organization, it may not be utilized in a way that conflicts with other laws that control the ability to contract.

An instance of Identity vis-à-vis capacity

1. The company has an independent identity under the Companies Act, of 1956.
2. Company can act only through individuals acting on behalf of the Company.
3. Such authorization or individuals acting would depend on specific provisions of the Companies Act 4. DSC may be issued to the company under the Act/Rules.
4. The use of DSC though valid under the Act would be governed and be subject to the Companies Act, 1956.

The Act allows for a corporation to be issued DSC. But there aren't any rules or recommendations that specify how to utilize this kind of DSC. As a result, even while a DSC is legitimately issued, it may be utilized in a way that renders it void under the Companies Act of 1956. As a result, the CA needs to carefully consider how the DSC will be used. Furthermore, the CA must make sure that any deemingprovisions in its Certification Practise Statement or other agreements minimize its liability for unlawful conduct.

(E) Cross-verification

A CA is not permitted to start operations unless it has made arrangements for cross-certification with other licensed CAs, according to Rules 12 and 20.

In a way, this clause can be interpreted as pressuring the CA sector to provide uniform guidelines to encourage the use of digital signatures. Nonetheless, it is illogical for anyone CA to begin operations unilaterally due to this clause. This cross-certification clause elevates the integration to a very high degree. This is due to the fact that the majority of Indian CAs are trusted by other international CAs.

Therefore, cross-certification in India would also include the creation of a certification chain amongst the various international companies.

It's interesting to note that the industry was taken aback by the final CA Rules because they included no such clause in either of the two draught versions. Although offering seamless authentication services is a commendable goal, the method by which it is being accomplished seems narrow-minded.

Currently, only an organization with a second CA-licensed license that shares the same vision for certification services may begin issuing DSCs.

Furthermore, it's unclear why cross-certification is required. When there are many trust levels (certificate kinds) or when there is no other way to guarantee trust except via dependency, cross-certification is usually necessary. Nevertheless, in the Indian context, there is no need for a formal arrangement because the trust is protected by legislation. Furthermore, it seems that the Act precludes the existence of many kinds of certificates. Therefore, it's unclear what this clause will actually accomplish.

(F) Suspension and revocation

The Act (***Section 37***) prescribes certain situations where a CA may suspend a DSC:

Upon request by the subscriber or any person authorized, or in public interest However, the Act also provides that no DSC may be suspended for a period exceeding 15 days, without providing an opportunity to the subscriber.

The Act (***Section 38***) and the CA Rules also prescribe certain situations where a CA may revoke a DSC: Upon request by the subscriber or any person authorized, or On the death of the subscriber, or Upon dissolution of the firm or winding up of the company While the aforementioned rules outline circumstances in which the CA "is authorized" to suspend orrevoke, this discretion would include a duty to guarantee that the proper suspension or revocation takes place.

In addition to the circumstances listed above in which the CA has discretionary authority, the CA has specific duties to withdraw a DSC under Rule 29 in the event that the DSC is compromised, abuse of the DSC, false information or mistakes in the DSC, and situations in which the DSC is not no longer necessary.

According to Rule 28, "compromise" refers, among other things, to a situation in which the DSC's private key is uncertain. There is uncertainty in the phrases "where the DSC is no longer required" and"misuse" of the Certificate.

Practically speaking, the CA would have to specify precisely what constitutes "misuse" and "expiration of requirement." This would necessitate a thorough recording of the agreements reached between the CA and all stakeholders, in addition to a thorough evaluation of what the real-world scenarios are.

In addition, the CA must do its best efforts to notify the parties involved as soon as such occurrences occur and has the authority to revoke the Certificate. The CA must include DSC information in its Certificate Revocation List upon revocation.

(G) Archives and Records

According to the CA Rules, all DSCs are to be preserved for a minimum of seven years or the length of time required by law. The definition of "the period of legal requirement" is somewhat vague and subject to several interpretations. In some circumstances, for example, copyright assignment (which isvalid for the author's lifetime plus 60 years), the signature on It could be necessary to preserve the assignment paperwork for over a century. Now picture the scene!Every CA would be sceptical if this uncertainty has met its responsibilities.

Rule 27 requires the Certifying Authority to maintain archives of:

- Applications for issue of DSCs;
- Registration and verification documents of DSCs;

DSC;

- Notices of suspension; Information of suspended DSC;
- Information of revoked DSC;
- Expired DSC. for a minimum period of 7 years or as per the legal requirement.

Schedule II's Guideline 9 mandates that the CA keep backups of certain important files, databases, and encryption keys, among other things. Guideline 6 specifies that the offsite backup must be safe and housed in India.

A general requirement under Section 30(b) is for the Certifying Authority to guarantee a fair degree ofservice dependability. Schedule III's Guidelines 9 and 10 control the upkeep of audit trails to confirm transaction patterns and have sufficient backups.

Equipment Signatures

These days, it's not unusual to receive automated responses from different web service providers. These can be offered via a variety of servers with a range of applications. Conventional automatic responses (like those for online orders) could equate to the signing of contracts.

Verifying that the order confirmations are genuinely from the online service provider is crucial since web-based communication methods are not impervious to outside intervention. Under such circumstances, it would be important to decide if the signature belongs on the equipment or on the person in charge of the device.

It follows that the signature cannot be entirely assigned to a piece of equipment since it lacks legal personality and decision-making ability. As a result, it seems that only individuals are eligible to get signatures. The relationship between the subscriber, the CA, and the equipment should be disclosed tothe person who depends on such a certificate. This would necessitate meticulous recording of the scope of obligations and hazards, as well as their restrictions.

Nonetheless, there would be a wide range of possibilities when it came to attributing an item's activities to the person operating it, considering the actuality and widespread use of programmable technology that can be told to behave in a specific way. Given that remote hacking instances seem to be becoming more frequent in this day and age, the owner or controller of the equipment may be more concerned about the "tamper-proof" quality of the device, making this more interesting.

Recognition of Foreign Cases

According to ***Section 19*** of the Act, the Controller may accept certificates issued by Foreign CAs(with the Central Government's previous permission and compliance with certain requirements).

Except for Rule 12(2) of the CA Rules, no rules have been released as of yet regarding the recognition of foreign CAs. According to Rule 12(2), before any cross-certification procedures between an Indian CA and a foreign CA are initiated, the Controller must expressly authorize the agreement.

If Section 19 of the Act recognized any DSCs, an individual in India would then have access to such DSCs. It seems that this usage would be limited, meaning that Indian citizens would only be allowed to depend on the DSC that is offered by the residents of another nation. But it doesn't seem conceivable that a native of India could acquire certificates from international CAs so that they may be applied to other transactions. If not, since all certifications may be requested for and awarded online, CAs wouldn't need to open a physical business location in India. In addition, the 49% foreigninvestment cap would not apply.

A person in India does not seem to be able to claim that he legitimately relied on a DSC issued by a foreign CA in the absence of such recognition.

Evidentiary Values of Electronic Signatures and Digital Signatures

(A) Secure Electronic Records

The amended Evidence Act offers advantageous provisions for secure electronic records and secure digital signatures.

Section 67A of the Evidence Act mandates that anyone wishing to rely on the fact that an electronic record has been digitally signed by a specific individual must provide proof of this fact unless the digital signature is secure.

In contrast to the requirement for explicit proof, ***Section 85B*** of the Evidence Act establishes an assumption that a secure record has not been altered until the moment at which it was validated.

Furthermore, the Section states that the information listed in a DSC is accurate, with the exception of specific nonverified subscriber information, and that the Court will assume in any proceedings involving a secure digital signature that the subscriber attached the signature with the intent to sign or approve the electronic record.

These assumptions have a significant influence on how business is conducted because they provide people the necessary push to rely on the seeming intentions of others.

Electronic recordings have been explicitly included in the definition of "evidence" since it was broadened. Additionally, remarks made in electronic formats may now be considered "admissions" under ***Section 17A*** if they imply any inference to a significant or in dispute fact.

Oral admissions about any document are not relevant unless and until the party proposing them demonstrates that (a) he is entitled to give secondary evidence of the contents of such document, or

(b) the authenticity of the document produced is in doubt. This is in accordance with ***Section 22*** of the Evidence Act. Furthermore, circumstances under which supplementary evidence pertaining to documents may be provided are outlined in Section 65. The Act's revision now includes ***Section 22A***, which applies the same regulation that applies to oral admissions to electronic documents as well.

The requirements for electronic record admissibility are covered in ***Sections 65A and 65B***. For example, Section 65B states that data included in an electronic record, whether it be printed or saved, would also be regarded as a document and admissible under specific circumstances.

A court will assume that any communication transmitted over an email server was fed into a machine for transmission, according to ***Section 88A***, which may be of special importance. However, the Court is not permitted to assume anything about the individual who sent the communication. It is only possible to evaluate the message sender based on the assessment of the available information, not on conjecture.

While emphasizing the parties' agreement may be appropriate, establishing a presumption of attribution in favour of any authentication procedures may not be appropriate because the security and dependability of these procedures vary so widely that there is no factual basis for establishing such a presumption.

(B) Secure Digital signatures

A digital signature is defined as "secure" ***in Section 15*** if, following the application of the security procedure, it is determined that the digital signature (a) was specific to the subscriber who applied it (b) was able to identify such subscriber (c) was created in a way or with a means that was solely under the subscriber's control, and (d) is nullified if the electronic record is altered. Although the concept of "digital signature" restricts the technique to asymmetric cryptosystems, the section as a whole appears to be somewhat broad. Since Section 3 already covers the requirements of uniqueness and logical association, it is unnecessary to repeat them here. The further requirements of exclusive control and tamper-proof nature found in ***Section 15*** are absent from ***Section 3***.

A positive presumption of "intention" is offered in relation to "secure digital signatures" by ***Section 85B*** of the Evidence Act. The subscriber must attach the secure digital signature with "the intention ofsigning or approving the electronic record," according to the presumption that the Court must make.

However, a digital signature supported by a DSC has certain additional advantages.

First of all, ***Section 85C*** establishes a crucial presumption regarding the "identity" of the subscriber. According to this Section, the Court must assume that all of the data provided in the DSC is accurate, with the exception of any unverified data. This assumption may be the foundation of a digital signature's evidential value and helps Additionally, the Evidence Act was amended to include Section 47A, which states that the CA's opinion is a significant fact when the Court is required to make a determination on a person's digital signature.

According to ***Section 67A***, it is necessary to substantiate that a digital signature, unless it is a secure digital signature, belongs to the subscriber if it is claimed that the subscriber's digital signature was attached to an electronic record. Furthermore, the person, the Controller, or the CA may be ordered bythe Court to produce the digital signature certificate in order to conduct such an evaluation. This seems to suggest that the CA is able to provide unsecured digital signatures.

But when one looks at the Act's overall structure, especially in Section 15 (which defines a "secure digital signature"), it seems unnecessary to establish such rules because all digital signatures would besecure.

Penalties And Offences

The Act has classified violations into two categories: those that are not strictly criminal, meaning they do not carry jail time penalties, and other violations.

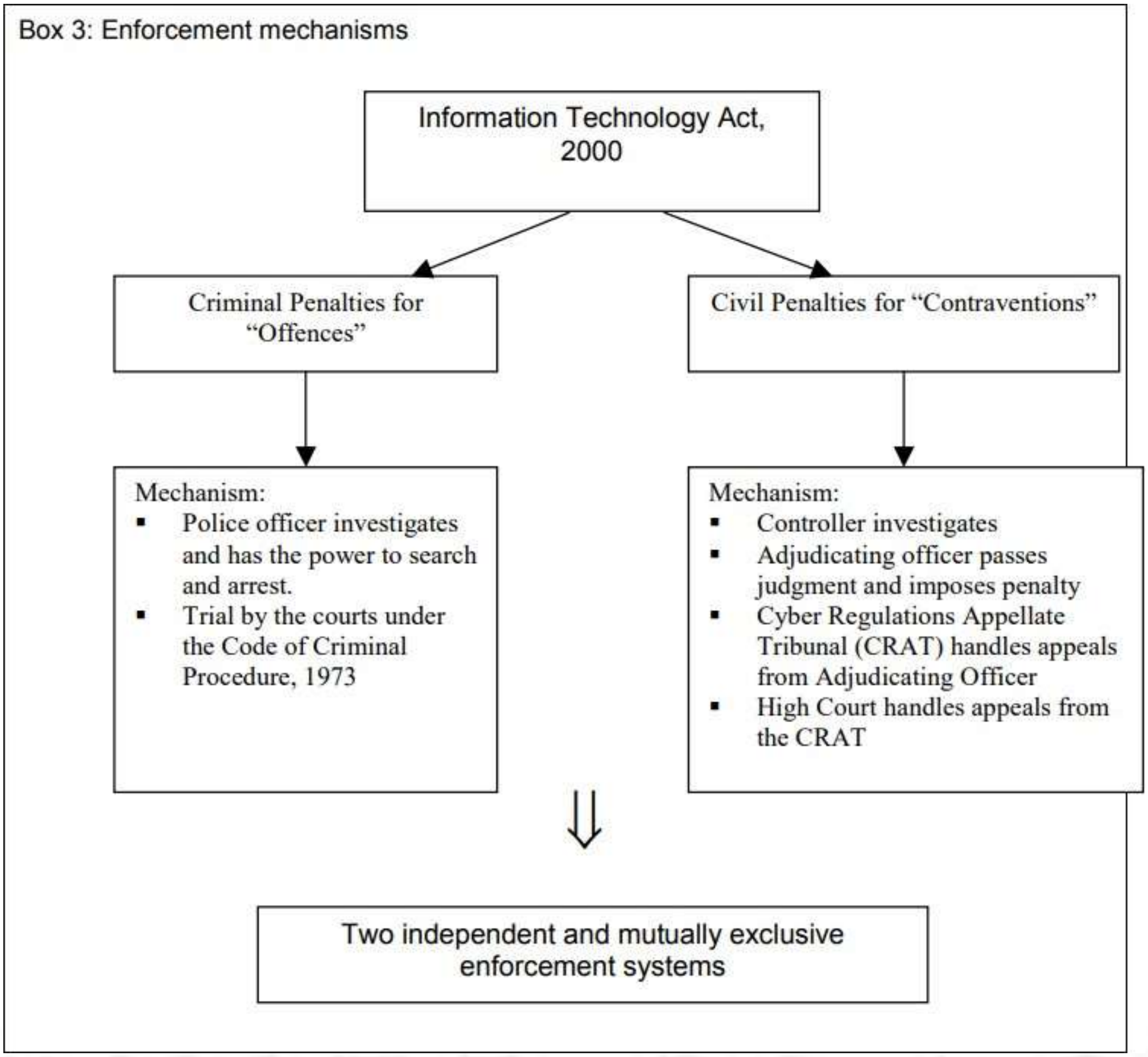
Several infractions are listed in Chapter IX of the Act, including unlawful copying, unauthorized access to documents, the introduction of "computer contaminants," denial of access, etc. Such a breach would include paying the impacted party's compensation as well as a monetary penalty.

A number of offenses are listed in Chapter XI of the Act, including altering source codes, hacking, publishing or transmitting pornographic material, fabricating information to get a DSC, publishing a fake DSC, and more. These carry both a financial fine and a jail sentence.

A portion of these infractions and crimes are predicated on the criminal intent or awareness of the individual committing the offense (such as altering computer source documents, hacking, or publishing digital signatures for deceptive purposes). However, some cases are solely founded on the performance of certain offenses, whether done so deliberately or innocently (publishing of false DSC, deception, violation of confidentiality, damage to computer systems, and electronic publication of offensive material). Men's rea is not a necessary component of some crimes, but it does exist from the traditions of criminal law, where courts are inclined to consider the criminal intent underlying a given behaviour.

Chapter XI of the Act, titled "Offences," deals with criminal offenses punishable by either a fine, a jail sentence, or both. Chapter IX of the Act, titled "Penalties and Adjudication," covers civil infractions that solely carry monetary penalties. Nevertheless, neither of these chapters' titles provides an explanation for this discrepancy. Moreover, both chapters contain allusions to criminal and civil infractions, and Chapter XI uses the terms "offense" and "contravention" interchangeably.

The Act aims to establish two unique and different procedures for handling misbehaviour: one appears to be for civil misbehaviour and the other for criminal misbehaviour.


Box 3: Enforcement mechanisms
Information Technology Act, 2000
Criminal Penalties for "Offences"
Civil Penalties for "Contraventions"
Mechanism:
Police officer investigates and has the power to search and arrest.
Trial by the courts under the Code of Criminal Procedure, 1973
Mechanism:
Controller investigates
Adjudicating officer passes judgment and imposes penalty
Cyber Regulations Appellate Tribunal (CRAT) handles appeals from Adjudicating Officer
High Court handles appeals from the CRAT
Two independent and mutually exclusive enforcement systems

Even while these procedures appear to be quite different from one another, the Act's wording is ambiguous about the kinds of infractions that fall under each mechanism, which leaves room for potential power overlap. There has been a vague and perplexing exchange of the terms "offence" and "contravention." It should have been evident from the Act's definitions of both terms that "offence" refers solely to criminal infractions and "contravention" refers only to civil infractions. The Act's current organisation makes it difficult to read because it does not explicitly distinguish between criminal and civil infractions, or vice versa.

These are a few examples of how the Act creates confusion and overlap in authority by using theterms "offenses" and "contravention" interchangeably.

- The terms "contravention" and "powers of the Controller" are used in a civil context in ***Sections 28, 29, 43(g), 45, 46, and 63***. These sections solely address monetary penalties as opposed to jail time. Additionally, the terms "offense" and "police powers" are discussed under Sections 33, 68, 78,and 80, which also entail criminal penalties.
- Nevertheless, the terms "offense" and "contravention" are used interchangeably and ambiguouslyin Sections 69, 70, 76, and 85. For instance:

The Controller may intercept information "for preventing incitement to the commission of any cognizable "offence"," as permitted by Section 69(1) of the "Offences" chapter. Although it is unclear if the phrase "offence" refers to criminal or civil infractions, one may assume that it would since the Controller would wish to stop either from happening.

In the 'Offences' chapter, ***Section 70***, the word "contravention" is used in a criminal rather than a civil sense. A person who uses a protected system "in contravention of the provisions of this section shall be punished with imprisonment," according to the statement. Although the phrasing is "in violation" rather than "contravention" as a noun, ***Section 43(g)*** reasonably uses a comparable phrase.

The word "contravention" is used quite broadly in ***Section 76***. This is covered in the "Offences" chapter as well, but as confiscation may be required in either situation, it seems to apply to both criminal and civil circumstances.

Section 85 is especially perplexing since, although being labeled "Offences by Companies," the section's content refers to "contravention" several times without mentioning "offenses." The terminology used in this section appears interchangeable, and it's not obvious if this relates to criminal or civil infractions or both.

The Act seeks to establish separate processes for civil and criminal adjudication in order to tackle violations falling within its purview. The two mechanisms were designed to have different capabilities from one another. Nevertheless, the Act falls short of its aim due to a misunderstanding in its terminology. Given that the words "offense" and "contravention" have been used synonymously, there may be similarities between the Act's civil and criminal procedures.

Section 28 of the Act grants the Controller the right to look into "contraventions," whereas S***ection 78*** gives police officers the jurisdiction to look into "offenses." The Act's goal of having two independentmechanisms for handling Act breaches is not suitably served by the lack of precise definitions for the words "offense" and "contravention," which leads to ambiguity and power overlap. The terms of the two mechanisms described in the Act should be differentiated if the mechanisms are to function without being subject to interpretational disputes.

Foreign Investment

Requirements for CA licensing applicants are outlined in Rule 8 of the CA Rules. A firm that is registered in India and has at least Rs. 50 million in net worth and paid-up capital is qualified to apply for a license. Nonetheless, no business seeking to apply for a license may have non-resident Indians orforeigners owning more than 49% of its stock.

Location Of Facilities

According to Rule 9, all infrastructure related to the creation, issuance, and administration of DSCs aswell as the upkeep of directories must be situated in India.

Many Indian firms sought partnerships with international CAs so that they could get licenses in India to issue DSCs and outsource their technological support or back-end operations. The precise scope of this provision (certificate server, directory server, key recovery server, etc.) is up for discussion. The Controller would have to make a decision about the legality of these types of collaborations as and when they are created. To minimize any uncertainty, it would be prudent for the controller to address these matters upfront.

Lifetime of DSC

Regarding the operating duration of the certificate, suggestions are given in the Security Guidelines (Schedule III appended to the CA Rules). Three years44 is the recommended duration for a subscriber's private key, under Paragraph 21 of the Security Guidelines. While the recommended duration for the CA's private signing key is two years, the recommended duration for the root keys and related certificates is five years.

Conclusion

To control the digital world in this new era of communication, appropriate, targeted, and effective laws must be adopted globally. Cyberspace jurisdiction is a highly complicated issue. Cyberspace is not subject to the ideas of territorial application of law and territorial character of law.

As a result, global legal standards and cooperation in the areas of substantive and procedural law must be adopted. In order to effectively manage cybercrimes and cyber violations, as well as promote good governance via electronic and mobile governance, we need to establish a set of procedures that will beadhered to by particular courts on a national and worldwide scale. Evidence-related problems play a part in the spread of cybercrimes and the increasing threat they pose. Cybercriminals are certain that it will be extremely difficult to apprehend them, and even if they are, the process of enforcing sanctions will be extremely problematic since the practical issue in cyberspace is proof.

After above discussion, we can conclude that the utility of digital as well as electronic signatures are asfollows:

Evidential value: When a digital signature is applied to electronic documents, the recipient has cause toassume that the communication or document was sent by a recognized party, was not altered during thetransaction, and should be regarded as legitimate. As so, it establishes the authenticity of the electronicrecord as documented evidence.

Proof of attached document: Although adding a digital signature or electronic signature to an electronic record is primarily used to validate the legality of certain other documents, it also serves as evidence ofany attached documents.

Authentic document execution: Although a digital or electronic signature is required for commercial transactions, the digital or electronic signature is crucial for the legal approval and authenticity of the document's execution.