ISSN.0973-3280

BANGALORE UNIVERSITY LAW JOURNAL

UGC approved Peer Reviewed
and
Refereed Journal

VOL : 9 NO. 1

JANUARY 2019

Vol. 9 No. 1

BANGALORE UNIVERSITY LAW JOURNAL

UGC approved Peer Reviewed and Refereed Journal

CITE THIS VOLUME AS 9 BULJ 2019 (1)

This Journal is published by

University Law College & Department of Studies in Law,

Bangalore University, Bengaluru

Price of single issue : ₹ 200/-

CALL FOR CONTRIBUTIONS

Bangalore University Law Journal is a biannual publication. Contributions to the journal are invited in the form of articles, notes and case comments.

Contributions should be typed in double space on one side of the A4 size paper and should also be sent by rewritable CD. It may also be sent through email-id buljulc2020@gmail.com

The Editors, Publishers and Printers do not claim any responsibility for the views expressed by the contributors and for the errors, if any, in the information contained in the journal.

The subscription amount may be sent to the following address along with D.D drawn in favour of Finance Officer, Bangalore University, Bangalore.

BANGALORE UNIVERSITY LAW JOURNAL
C/O **PROFESSOR DR. V. SUDESH**
PRINCIPAL
UNIVERSITY LAW COLLEGE
BANGALORE UNIVERSITY, BANGALORE

EDITORIAL NOTE

It is indeed a momentous occasion for Bangalore University in general and University Law College in particular to bring out a Law Journal after completion of more than 50 years of its existence under the auspices of Bangalore University. The editors wish to place on record and thank V. B. Coutinho Trust ® for being kind and gracious to hand over the future publications of Bangalore Law Journal (BLJ) to the Principal, University Law College, to be published as "Bangalore University Law Journal" (BULJ). We also thank the Hon'ble Vice-Chancellor, Registrar and Finance Officer, Bangalore University, Bangalore for having accepted our proposal for the journal and sanctioning requisite funds for printing of the journal.

Research is an important aspect of the academic life of a teacher. The ever changing socio-legal dynamics present an opportunity to all the teachers to undertake research by writing scholarly articles on several issues and thereby contribute in furthering knowledge and promote future research.

It has been a long standing desire of the faculty of University Law College & Department of Studies and Research in Law, Bangalore University to have a journal of its own and we are happy that it is fulfilled with the blessings of Jurists, Senior Professors and Former Principals of University Law College, Bangalore University, Bengaluru.

The BULJ will be a peer reviewed journal inviting scholarly articles from faculty and scholars across the country. We hope the inaugural issue of BULJ would benefit the readers.

Prof. Dr. V. Sudesh
Principal
University Law College
Bangalore University, Bangalore

CONTENTS

774

Sl No	Particulars	Page Nos
1	Is Sexual Harassment in Higher Education Institutions a Myth or Reality? A Legal Study *-Prof. (Dr.) T.R.Subramanya and Ms. Arunaa J.*	1-16
2	International Rivers: Challenges Posed by the Threat of Climate Change to India and Her Neighbours *-Shri. Mohan V. Katarki*	17-26
3	Cyber Security Laws Regulating E – Commerce Sector in India *-Prof. Dr. Suresh. V. Nadagoudar and Ravindra K. Rajput*	27-36
4	Revisiting the Ancient Idea of Corporal Punishment in Schools: In the Best Interest of the Child *-Dr. Kim Rocha Couto*	37-52
5	The Myth of Legal Protection of Women Workers in the Construction Sector: An Analysis of the Land Mark Judicial Developments *-Dr. Sapna S*	53-72
6	Law Relating to Conservation and Management of Forest Resources in India: An Analytical View *-Dr. Aneesh V. Pillai*	73-87
7	Child Labour Hampered the Development of Nation: Issues and Challenges Ending Child Labour in India *-Dr. Janhavi S S*	88-96
8	Right to Safe Food in India - An Unending Litany *-Dr. N. Sathish Gowda & Sumithra. R*	97-114
9	Montevideo Programme: As an Action Plan *-Dr. Jyothi Vishwanath and Sumanth H.M*	115-120
10	Legal Regime on Human Trafficking in the Dark Net in India: An Analysis *-Dr. Chandrakanthi L. and Tito Paul*	121-141
11	Women Empowerment in India: An Overview of 73rd Amendment *-Dr. C.R Jilova*	142-148
12	Rights of Female Prisoners under Indian Constitution: An Analysis *-Dr C.B. Ranganathaiah*	149-155

nal water whether by treaty or judicial allocation, can be reopened nged circumstances (*rebus sic stantibus*)[19]. Therefore, India and her rs China, Nepal, Bangladesh, Bhutan and Pakistan, must actively on the issues of climate change and its impact on the waters of rnal rivers. A regional cooperation is the need of the hour for India, Nepal, Pakistan, Bhutan and Bangladesh. The Mekong River sion, established under the Mekong Treaty, has developed a program, the "Climate Change and Adaptation Initiative"[20]. A similar nt Commission must be established by a treaty amongst India, China, lesh, Bhutan, Nepal and Pakistan to address and guide them on climate and its impact on water resources sourced from Himalayan glaciers nsoon, since both the sources are clearly at risk due to global warming.

usions

The international community, through the UN, responded to the threat nate change in the 1980s as a precautionary measure. Over decades, the of threat of climate change due to global warming and its cascading on water resources, crop water requirement, soil moisture, *etc*., has ced to a serious level, which cannot be ignored. The Paris Agreement in commits the international community to pursue their efforts to limit l warming to 1.5°C above the pre-industrial limit. The flows of IGB e depending on Himalayan glaciers and monsoon are at risk from global ting. The IPCC studies based on GCM are inadequate to face the threat imate change and its impact on water resources in IGB basins. The ections at the global level must be translated into regional predictions by nscaled models for better preparedness. The India, Pakistan, Bangladesh, al, China and Bhutan, as basin States, owe an obligation to each other to tutionalize and conduct downscaled studies to face the threat of climate nge and its cascading impact on water resources of IGB basins as the mon concern of mankind as mandated by UN in the 1980s.

Mohan. V. Katarki, If Climate Change is a Possibility, Will There be a Reallocation of International Waters (page 83, Inter-State & International Water Disputes. Edited by P. Ishwar Bhat, Published by Eastern Book Company, 2013) https://www.mrcmekong.org

CYBER SECURITY LAWS REGULATING E-COMMERCE SECTOR IN INDIA

Prof. Dr. Suresh. V. Nadagoudar[*]
Ravindra K. Rajput[**]

Introduction

As it is said, in the present world nothing comes without a cost and in business world, online shopping or e commerce is not an exception to this. A customer has unlimited choice over this platform, he can fall a victim to the choice which is made available to him and we see that a customer spends a good amount of time on this platform without making any final decision.

In e-commerce one of the major options for purchase from the Internet is that, goods can be bought through debit card, credit cards, payment gateway platforms such as Paytm, PayPal, *etc*. It is thus quite possible that such customers may fall prey to security and privacy issues when shopping online.[2] However, with the option of COD (Cash on Delivery) the issue of privacy and security can be seen solved to certain extent as the customer who opts for COD may not be required to forgo personal details, however, still the threat of defect in goods or deficiency in service persists in an online purchase transaction.

In the recent times the internet has grown as an important component for quick and rapid purchase revolution which has breached into the busy lifestyle of the consumers. Whether it is for the purpose of communication or exploration, connecting with people or any official work, Internet is the go to tool for all this activities. With all these advancements the consumers are now turning more and more towards e- commerce for buying of goods at an affordable price[3]. Thereby, what we see is that, with the growth of internet it

[*] M.A., LL.M., Ph. D, Professor, University Law College & Department of Studies in Law, Bangalore University, Bengaluru.
[**] Research Scholar, University Law College & Department of Studies in Law, Bangalore University, Bengaluru & Asst. Prof. SDM Law College, Mangaluru.

[1] Saher Owais Talib, "E-commerce laws and regulations in India", Volume 3, Issue 4 International Journal of Multidisciplinary Research and Development, p. 66-67 (2016), *available at*: http://www.allsubjectjournal.com/archives/2016 /vol3/ issue4/3-4-30 (last visited on June 17, 2020).
[2] *Ibid*
[3] *Ibid*

has led to the growth of new developments such as e commerce, internet of things, Artificial intelligence, etc

The customers like never before are buy goods and availing various services on the e commerce platform Till recently, people used to book train, air or movie tickets online, but now they use it to purchase electronic, clothing, home and kitchen items, grocery and household supplies and beauty and health products and the list goes on This change has happened due to the fact that people have realized the convenience and most importantly time saving factor, added with discounts and deals available online.[4] This has led the people from traditional physical stores to a virtual store Thus, what we see is that, to reach and target such tech savvy consumers, a fierce competition is seen amongst e commerce tech giants on the web

E-Commerce as a concept has evolved and developed in nations such as United States These nations have put in place appropriate laws and enough infrastructure to deal with the needs of online consumers. This has helped the consumers not only to be secure by complying with the laws of these nations but also helping the nation in increasing its GDP.[5]

E-Commerce in India can be seen from a totally different prism. It has embedded within it all the advantages of commercial viability and profit making However, on the regulation front, we do not see a dedicated e-commerce law, although we have the Information Technology Act, 2000, which is based on UNCITRAL (United Nations Commission on International Trade Law) model law.[6] The main purpose of this law was to grant legal recognition to all transactions which were done through electronic data exchange or by other means of electronic communication or e-commerce, replacing the earlier paper-based communication.

Regulating the e-commerce business in absence of one dedicated law has led to different agencies to intervene to regulate their activities, such as Enforcement Directorate (ED), SEBI and Competition Commission to protect the interest of the nation and consumers. Few major complaints have been in regards to quality, purity, price, unfair trade practices and predatory pricing

4 *Supra* note 1
5 *Ibid*
6 *Ibid*

tactics followed by the Indian e-commerce giants Hitherto to ascertain extent, the Information Technology Act, 2000 and The Consumer Protection Act, 1986 protects the consumer against their unscrupulous exploitation

I. Types of E-Commerce Facilities

Electronic commerce or e-commerce consists of the buying and selling of goods and servicing of products or services over computer networks The Information Communication Technology (ICT) businesses may see this as an electronic business application aimed towards commercial transactions

An alternative definition of electronic commerce may be viewed as the conduct of business which involve commercial communications and management using electronic methods, such as electronic data interchange and automated data-collection systems.

There are six types of E-commerce/e-business types:

i Business to Business (B2B)
The Business to Business is the one of largest e-commerce model Here, both the sellers and buyers are business entities. In this model the transactions are basically between a retailer or a wholesaler or a manufacturer and wholesaler. Further, the transactions of B2B business model are much higher than that of B2C model.
Example: Alibaba; Amazon business, Boeing, India-mart, to mention a few[8]

ii Business to Consumer (B2C)
The B2C business is the most popular and predominant model In this online model, the business sells goods directly to individual customers This business model provides a direct interaction with the customers
Example: Flipkart, Amazon; Myntra, etc.[9]

iii Consumer to Consumer (C2C)
The consumer to consumer or C2C business model involves a transaction between two consumers, i e citizen to citizen. The best example of this model would be online auctions wherein a customer or visitor or seller posts an item for sale and other customer or potential

Ibid
6 Types of E-commerce Business Models, available at: https://www.rapportrix.com/6-types-of-e-commerce-business-models (last visited on June 17, 2020)
Ibid

buyer bids to purchase it. However, in such transactions the third party generally charge a commission. Normally, C2C business requires immense planning and marketing knowledge as these sites act as intermediaries to bring the customers together.

Examples: eBay, OLX, etc[10]

iv. Consumer to Business (C2B)

The Customer to Business or C2B model involves customers selling their products or services to business. It is a typical model where a sole proprietorship/ entrepreneur are serving larger business. What differentiates C2B from other business models is that the value for the products is created by the customer and this caters to the needs of freelancers, who fulfil the given needs of their clients. In addition to this we see customers provide advertisements/reviews to goods or services in exchange of money.

Example: An influencer advertising the products of a company amongst his followers.[11]

v. Business to Administration (B2A) / Business to Government (B2G)

The Business to Government (B2G) is also referred to as Business to Administration (B2A) commerce. Here we see the government and business houses use central websites to do business with each other. This can be seen in public sector marketing, which means providing products and marketing services at multiple government levels. In this model, the business groups can bid on government opportunities, such as tenders auctions; online application submissions and providing IT support to the local government bodies.[12]

vi. Consumer to Administration (C2A)/ Consumer to Government (C2G)

The Consumer to Administration (C2A) or Consumer to Government (C2G) model enables the consumers to post feedback for the service/facility provided by the government or request for information in regard to public sectors services/facilities directly to the government administration or authorities' websites.

Example: payment of electricity bill, payment of health insurance, payment of taxes, etc.[13]

[9] *Ibid*
[10] *Ibid*
[11] Supra Note 8

777 6

II. E - Commerce and Security Issues

The assets generated in E-commerce need to be protected from unauthorized use; unauthorised access, alteration or destruction of their data. Due to security issues the consumers fear the loss of their confidential information and e-commerce businesses fear to the loss due to break-ins. We see a great number of issues associated with e-commerce security, be it social or authoritative in nature. In regards to authoritative process we need to develop a proper chain of management for interconnecting security policies and its implementation through security tools. Further, it is often seen that in security lapses it is either the employee or users who are weak, rather than the technology, leading to security breach. One of the major problem or concern is the lack of willingness amongst the users to adhere to basic security practices or guidelines when using e commerce facilities. Example: Storage of passwords in unencrypted files; do not update their operating systems or browsers; etc.

A few security issues involved with e-commerce are as follows:

i. Denial of Service: In a denial-of-service (DoS) attack the legitimate users are not allowed to access the information systems, devices, or other network resources because of the actions of a cyber threat actor. The various forms of services that could be affected are websites, e-banking facilities and other services that depend on affected computer or network. In a denial-of-service attack the targeted host or the network is flooded with huge traffic till the target cannot respond or simply crash thereby preventing the access to a legitimate user. These attacks affect the e-commerce business both in terms of time and money as their resources and services are not accessible to the consumer. DoS attacks have grown into a complex and sophisticated attack as "distributed denial of service" (DDoS) attacks.

ii. Unauthorized access: In case of unauthorised access a person obtains logical or physical access to a computer system, its network, the applications and data involved or any other resource , without due permission.

iii Credit card fraud: In recent time's Credit card fraud are the most common security threat faced by online retailers. This occurs when a cracker/hacker gains unauthorized access into customers personal as well as payment data. To access this, the hacker may force himself into the database of an e-commerce site with a help of malicious software programs. The data collected is often seen sold in the black market

iv. Phishing Scams: E-commerce sites are not immune from phishing scams. With the use of social engineering, consumers may be lured to online shopping sites, through emails sent from known or unknown people and target the login credentials and credit card numbers, by forcing them to click a link which resembles e-commerce site.

III. Security for E-Commerce Applications

To counter the security issues few best practices can be adopted are as follows:

i. Encryption: Encryption of data is a mode of scrambling data whereby only sanctioned parties can understand the information provided. In technical sense, it is the process where a plain text is converted into a cipher text. In simpler terms, it is a process where readable data is altered to appear in random. This process requires a key, a set of mathematical values (an algorithm), which is available with both the sender and recipient of message. This process helps to secure stored information and in secure information transmission.[14]

ii. Secure - Hypertext Transfer Protocol (S-HTTP): The Hypertext transfer protocol secure (https) is a secured version of HTTP. It is a primary protocol that is used to transmit data between the website and a web browser. HTTPS is always encrypted so as to increase the security of data transfer. Why is it important in e-commerce, because in an e-commerce website the consumer transmits sensitive data such as login credentials, banking details, purchase history, etc.[15]

iii. Digital Signature: A digital signature can be said as an electronic equivalent of a individuals physical signature. It is a mode that provides guarantee to the users that information has not been modified or tampered with. This helps in verifying the identity of the organization or an individual. Normally, digital signature is a hash of the message, which is encrypted, with the help of a public key and private key. These signatures are basically used to authenticate a website or to establish an encrypted connection between users.[16]

iv. Digital Certificate: A Digital certificate is an electronic credential which binds the identity of a certificate owner to a pair of encryption keys, one public and one private, which are used to encrypt and sign data/ information digitally. A digital certificate ensures that the public key obtained in the certificate belongs to the individual to whom the certificate has been issued and thereby verifies that the individual sending a message is one who he claims to be. Normally, a digital certificate is issued by an authorised third party institution known as certification authority. The certificate contains the name of the company or the entity, the public key, a serial number allotted to the digital certificate, an issuance and expiration date, the digital signature of the certificating authority and any other identifying data.[17]

These best practices need to be adopted in order to maintain data confidentiality; help in authentication and identification of service providers and users; to have access control; to maintain the integrity of the data and see to it that there is non-repudiation of data.

IV. Cyber Security Laws and Policies regulating E – Commerce in India

The latter half of 90's saw tremendous growth in globalization and computerization. Countries computerised their governance systems and e-commerce saw enormous growth. Whereas, International trade and transactions till then were predominantly done through documents transmitted either by post or telex only. Similarly, in the administration of justice, evidences and records were paper based. However, with International Trade accepting electronic communication, and with email gaining momentum, a need was felt to recognize electronic records that are the information stored on a computer or an external storage.

In this regard, a Model Law on e-commerce was adopted in 1996, known as United Nations Commission on International Trade Law (UNCITRAL). In January 1997, the General Assembly of United Nations passed a resolution, recommending all the nations of the United Nations to give favourable considerations in adopting the said Model Law, which provides for recognition to electronic records.

The Government of India in order to facilitate e-commerce and provide legal recognition to electronic records and digital signatures realized the need to introduce a new law and make suitable amendments to the existing laws.

---

[14] Santosh Kumar Maurya and Nagendra Pratap Bharati, "Cyber Security; Issue and Challenges in E-Commerce" available at: https://www.worldwidejournals.com/paripex/recent_issues_pdf/2016/January/January_2016_1453357435__63.pdf (last visited on June 17, 2020)

[15] *Supra* Note 14

[16] *Ibid*

[17] *Ibid*

This led to the enactment of Information Technology Act, 2000 (I T Act). In India, we see cyber laws embedded in the Information Technology Act, 2000. The Act provides a legal infrastructure for e-commerce and thereby having a major impact on e-businesses and the growth of new economy in India.

Under the I T Act, in regards to criminal offences that could be committed in e-commerce may be under the following offences:

i. Unauthorised access (hacking): The offence of hacking is covered under section 43 and 66 of the I T Act, it states that any person accesses a computer or computer system without due permission commits an offence under section 66 he shall be punishable with imprisonment for a term up to 03 years or fine up to 05 lakh rupees or both.[18]

Example: If an employee of a company (e-commerce giant) who has access to the confidential data and survey reports, helps a competing company gain access to this information through their network, then he shall be liable for the wrong of providing unauthorised access and thus liable.

ii. Denial of Service: The offence of Denial of service is covered under two provisions, Section 43(f) and section 66F of the I T Act, wherein the earlier provision is a general law applicable in cases of DoS, where as the latter section is applicable in cases of DoS which is in the form of a cyber terrorism act. The punishment for offence under section 43(f) is imprisonment up to 03 years or fine up to 05 lakh rupees or both and in case of section 66F it is imprisonment up to imprisonment for life.[19]

Example: The hackers look out for the loopholes in the app software or web based server software to either crash it or hang the application or they may make the servers so busy that legitimate request connections would fail thus denying the customers access to the site and in turn affect the business of the e commerce companies.

iii. Phishing / Identity theft / Fraud: The offence of Phishing is covered under sections 66C, 66D and 74 of the I T Act. Section 66C provides for prosecution of a person for phishing attacks or identity theft and shall be punished with imprisonment up to 03 years and fine upto 01 lakh rupees. Section 66D covers for acts where there is cheating by personation and shall be punished with imprisonment up to 03 years and fine up to 01 lakh rupees. Section 74 deals with creating fraudulent

[illegible] Cyber security 2020, available at https://clg.com/practice-[illegible]

e- signatures and certificates and shall be punished with imprisonment up to 02 years or with a fine up to 01 lakh rupees or both.[20]

Example: A hacker pretends to be e-commerce company to the customer who already is a subscriber of it by sending a email and then the hacker may request for personal data or install a malware, and the customer thinking it is the e-commerce company, interacting with him, may share the data or click on a link for offers and thus installing the malware and become a victim of phishing.

iv. Breach of confidentiality and privacy : Section 72 and 72A of the I T Act, deal with breach of confidentiality and privacy and disclosure of information in breach of lawful contract. The punishment under section 72 is with imprisonment up to 02 years or with a fine up to 01 lakh rupees or both and in case of section 72A it is with imprisonment up to 03 years or with a fine up to 05 lakh rupees or both.[21]

Example: The customer in order to purchase a product on an online platform may provide his credit card details. Here if the card details are leaked out in public domain in breach of confidentiality agreement, the person who leaks such information shall be held liable.

v. Data Protection : In cases of failure to protect data, section 43A of the I T Act, states that the corporate body shall be liable to pay compensation appropriately, if it is negligent to implement and maintain reasonable security practices and procedures.[22]

Example: The e commerce entities deal with lots of data, be it users profile, their choice of purchases, payment details etc. Here the company owes the duty to protect such data, in case of breach of data protection, the entity will be held liable.

In addition to the provisions above stated, under the Information Technology Act, 2000 in furtherance of cyber security measures, various security standards and procedures have been created under the rule making power of IT Act, such as: The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 to mention a couple of them. In addition to these rules there are sectoral cyber security

[illegible] *supra* note 18

related compliance regulations such as for banks and non banking financial institution

Further, the National Cyber Security Policy, 2013 is an evolving task and it caters to the whole spectrum of Information and Communication Technology (ICT) users and providers including home users and small, medium and large enterprises and government and non government entities. It serves as an umbrella framework for defining and guiding the actions relating to security of cyberspace

Conclusion

E commerce as a business model is connected with various sections such as Information Communication Technology, banking, retail, manufacturing, import and export, foreign direct investment, consumer protection and so on, and due do this interconnection of e -commerce with a variety of sectors, numerous laws, rules and regulations are applicable in this regard and this has created a daunting task for law makers and law enforcement agencies, especially in respect of maintaining the cyber security standards on par with international standards. With flaws and loopholes in the law and lack of strict enforcement of these laws, the cyber offenders get away, only to leave the consumers or e-commerce business enterprises victim of various cyber crimes and a mere spectator of these acts.

These concerns have reached at the highest level of Indian government and in this regard draft e-commerce law/ policy for India are being looked into. In addition, under the new Consumer Protection Act, 2019; draft E-commerce Rules under the said Act is been discussed by the law makers. The Personal Data Protection Bill, 2019 seeks to provide for protection of data and privacy of individuals, which could be seen applicable in e commerce as well. With all these new laws, rules and regulations being in the process of enactment, there seems to be a positive intent from the law makers to cater to the need of adequate cyber security in e-commerce.

Prevention is better than cure, thus, self regulation remains to be one of the strongest deterrence against cyber crimes in e-commerce as fraudsters are trying to take advantage of ignorant and errors made by online shoppers. As the authors firmly believe that a dedicated e-commerce law for India is in need of the hour and amending the IT Act, 2000 to house e-commerce related issues is not a good option and it should be the last option of the law makers.

RE-VISITING THE ANCIENT IDEA OF CORPORAL PUNISHMENT IN SCHOOLS: IN THE BEST INTEREST OF THE CHILD

*Dr. Kim Rocha Couto**

Children are sick of being called 'the future'. They want to enjoy their childhoods, free of violence, now"
Paulo Pinheiro

Introduction

Children are the future of the nation. They are also among the most vulnerable sections of society. Development of the child in a safe, secure and conducive environment is in the best interest of the child and crucial for the holistic growth of the nation. Children must have access to such an environment at home, at school and in their neighborhood. Since a child spends much of his time at school in his formative years, it is imperative that the school in which he is placed presents an environment free of the threat of corporal punishment, which facilitates the learning of subjects, skills and values.

Interestingly, one finds that education in ancient India had its focus on the intellectual development and character building of the learner. The twin objective of the traditional system of learning was to create useful and good persons in society. In the case of a delinquent learner, the punishment was meted out with the objective of self-reform, implying the correction of unrighteous behaviour. Observances of fast and such other spiritual modes of atonement by erring students were generally advocated for the purpose. To quote from a verse in the Manusmriti "*Let him punish first by (gentle) admonition, afterwards by (harsh)reproof, thirdly by a fine, (and) after that by corporal punishment.*"[1]

In contemporary times, the teaching-learning environment in schools has undergone several changes. The use of corporal punishment on school children is slowly becoming ubiquitous.[2] In addition, physical punishment

* Assistant Professor, V.M. Salgaocar College of Law, Miramar, Goa

1 Available at https://www.sacred-texts.com/hin/manu/manu08.htm(last accessed on 15/2/2019