Legal Regulation of E-Commerce: A Study with Reference to Consumers' Rights

THESIS

SUBMITTED TO THE
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करूणा
ESTABLISHED 1996

FOR THE AWARD OF THE DEGREE OF

Doctor of Philosophy

SUPERVISOR
PROF. SUBIR K. BHATNAGAR
DEPARTMENT OF HUMAN RIGHTS

SUBMITTED BY
DEEPENDRA NATH PATHAK
ENROLLMENT NO.- 106/08

DEPARTMENT OF HUMAN RIGHTS
SCHOOL OF LEGAL STUDIES
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A CENTRAL UNIVERSITY; NAAC- 'A' GRADE)
VIDYA VIHAR, RAEBARELI ROAD, LUCKNOW-226025 (U.P.), INDIA

2021

Dedicated
to
My Beloved
Father & Mother

DECLARATION

I, **Deependra Nath Pathak,** hereby declare that this research work embodied in this Ph.D. thesis titled **'Legal Regulation of E-Commerce: A Study with Reference to Consumers' Rights'** has been carried out by me under the supervision of **Prof. Subir k. Bhatnagar (Retd.),** Department of Human Rights, School of Legal Studies, Babasaheb Bhimrao Ambedkar University (A Central University) Lucknow, 226025.

This Research work is an original work and it has not been previously submitted in part or full for any other degree or diploma in this or any other university. This is also declared that the thesis is essentially free from all kinds of plagiarism.

Dated: 28.06.2024

Place:

(Deependra Nath Pathak)
Research Scholar
Enrollment No.-106/08
Department of Human Rights
School of Legal Studies
Babasaheb Bhimrao Ambedkar University
Lucknow-226025 (U.P)

BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
LUCKNOW
प्रज्ञा शील करुणा
ESTABLISHED 1996

बाबासाहेब भीमराव अम्बेडकर विश्वविद्यालय
(केन्द्रीय विश्वविद्यालय)
विद्या विहार, रायबरेली रोड, लखनऊ–226025
BABASAHEB BHIMRAO AMBEDKAR UNIVERSITY
(A Central University)
Vidya Vihar, Raebareli Road, Lucknow-226025

Letter No:………….

Date:………………..

CERTIFICATE

This is to certify that the thesis titled **'Legal Regulation of E-Commerce: A Study with Reference to Consumers' Rights'** submitted by **Mr. Deependra Nath Pathak** is an original research work and has not been previously submitted in part or full for the award of any other degree or diploma to this or any other university.

This thesis submitted to Babasaheb Bhimrao Ambedkar University, Lucknow satisfies all the requirements as stipulated in the *Doctor of Philosophy (Ph.D.) regulations, 1999 as amended in 2013* and it is fit for submission and evaluation for the award of the degree of Doctor of Philosophy of the University.

Date: 28.06.2024

Place:

Supervisor

SKBh
28.6.2024

Prof. Subir K. Bhatnagar (Retd.)
Department of Human Rights
School of Legal Studies
B.B.A.U., LUCKNOW

28/06/2024

Head
Department of Human Rights
School of Legal Studies
B.B.A.U., LUCKNOW

ACKNOWLEDGEMENTS

*First and foremost, I would like to praise and thank **God**, the almighty, who has granted countless blessings, knowledge, and opportunity to me, so that I have been finally able to accomplish the thesis.*

On the occasion of submission of this research work, first of all, I would like to record my sincere thanks to the authorities of Babasaheb Bhimrao Ambedkar University, who has not only permitted me to submit this thesis but also provided all research facilities.

*I would like to express my sincere gratitude to my advisor **Prof. Subir K. Bhatnagar (Retd.),** Department of Human Rights, School of Legal Studies for the continuous support of my Ph.D. study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. Your insightful feedback pushed me to sharpen my thinking and brought my work to a higher level. I could not have imagined having a better advisor and mentor for my Ph.D. study.*

*Besides my supervisor, I would like to express my deep sense of gratitude to prominent, **Prof. Preeti Mishra,** Head of the Department of Human Rights, School of Legal Studies, BBAU Lucknow, for encouraging me in completion of this research work. In spite of her busy scheduled, she has always been available to providing me mental support and valuable guidance every time when I needed.*

*I enthusiastically express my thanks to her generous behavior and inspirations. I am also thankful to **Prof. Priti Saxena**, Department of Human Rights, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow, for her insightful comments, determined encouragement and wise counseling in my crucial time. My sincere thanks also go to **Dr. Shashi Kumar**, Associate Professor & **Dr. Rashida Ather,** Assistant Professor, Department of Human Rights, School of Legal Study BBAU, Lucknow, without their precious support it would not be possible to conduct this research.*

I would like to acknowledge respected ***Prof. Sudarshan Verma*** *(Dean, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow) for providing moral support and all of the opportunities I was given to further my research.*

I would like to thank the Babasaheb Bhimrao Ambedkar University, Lucknow where I spent my research period for all the institutional support that I received over the years.

I am also grateful to the staff of the Library, B.B.A. University, Library Lucknow University, Library, RML National Law University, Lucknow for allowing me access to the material stocked therein. I have always been received immense help and inspiration from many institutions and individuals. Therefore, I express my heartiest gratitude to them. Researcher would like to forward thanks towards the non-teaching staff of the department for their Support.

I would like to record my thanks to all fellow research scholars, Department of Human rights as well as Department of Law, school for Legal Studies BBAU, Lucknow for their valuable suggestions, stimulating discussions and cooperation regarding my research work. I am also very much thankful to all my friends for providing me encouragement and love along with all fun.

Researcher puts special thanks and indebts to all authors, writers whose work has been utilized by the researcher in this present research study.

I am also thankful to ***Satyendra Kumar Maurya*** *(Research Scholar),* ***Maninder Kumar Singh*** *(Research Scholar),* ***Pramod kumar*** *(Research Scholar)* ***Dr. Munish Swaroop, Bhanu Pratap Singh Chauhan*** *(Advocate, Lucknow High Court) and my senior* ***Dr. Vijay Bhasker*** *who always encourages me and always provides mental support.*

I am also very thankful to my guardian respected ***Mr. Vishnu Narayan Misra*** *for providing me all help throughout all the crucial time and for his mental support. I put huge thanks to him for his honest cooperation throughout my life.*

Finally, I dedicate my all feelings of love and respect to my dear mother and father and my grandfather for shaping my life in the right way and they always inspired me to serve society and country. I always get their blessing from them to achieve success in my life. My parents taught me that the key component of life is to be rational, progressive and merciful. This accomplishment would not have been possible without them. This thesis stands as a testament to your unconditional love and encouragement.

Last but not the least I beg forgiveness of all those who have helped me and whose names I have failed to mention.

Deependra Nath Pathak

PREFACE

One of the most fascinating developments due to technological advancements has been the growth of electronic commerce commonly known as e-commerce, internet commerce or e-com. E-commerce has been generally defined as buying and selling of goods and services over electronic systems such as the internet and other computer networks. However, the term may refer to more than just buying and selling of goods and services online. It also includes the entire online process of developing, marketing, selling, delivering, servicing and paying for products and services.

E-commerce in India is still in the emerging stage however the most-pessimistic projections indicate a boom. It is believed that the low cost of personal computers, a growing installed base for Internet use, and an increasingly competitive Internet Service Provider (ISP) market will help fuel e-commerce growth in Asia’s second most populous nation. The amount of trade conducted electronically has grown extraordinarily. There is a growing awareness among the business community about the opportunities offered by e-commerce. The present research study has been conducted to provide a legal umbrella with an understanding of the Indian consumers who participate in the e-commerce market.

The research study has focused to evaluate the perceptions of e-consumers towards the present legal scenario governing e-commerce. It has also attempted to identify the difference in perceptions of online consumers and traditional consumers. In the research study the internet data, the risk associated with cyber space of the e-consumers like online fraud, cyber tort, hacking, etc have also been analyzed. Furthermore, the research undertakes the analysis of the impact of online shopping on the web and internet usage behaviour of e-consumers in different aspects. The present research has also analyzed the online usage behaviour of e-consumers in order understand their adoption of new technology. Finally, the research has discussed as to how the findings can be useful for the e-consumers in reshaping their strategies for better acquisition and retention of e-consumers with different backgrounds and perceptions. The entire study has been divided into seven chapters. Each chapter presents a focused discussion that has been systematically as well as logically organized to facilitate readability and comprehension.

The research study has also focused on social media policy 2021 and role of digital currency in e-commerce and their impact on e-consumers.

Chapter one focused on the introduction of the research study wherein the concept of e-commerce has been discussed in detail. The concept of e-commerce has been discussed both in the light of technological developments at the global level as well as to the Indian scenario. The chapter gives an in depth account of theoretical underpinnings building to understand the concept of e-commerce. In this chapter, the literature on the theme 'e-commerce' and its legal adoption has been discussed. As a broad number of research papers, books, reports have been analyzed and a comprehensive review has been done on the subject matter.

Research design, hypothesis and methodology forms a basic part of any research study. The successful completion of any research is dependent on the right selection of research methods and techniques to collect necessary facts, figures and data/information. Chapter one presents the aspects of research design and methodology viz. justification of the study, objectives and hypotheses of the study, the scope of the study, and finally limitations and future scope of research.

Chapter two titled *'E-Commerce: A Conceptual Analysis'* gives a basic exposition of the history and concept of e-commerce as well as a short discussion on the nature and functions of e-commerce, with figures to show present e-commerce user data to inform a comparison regarding the fundamental characteristics of e-commerce and has been analyzed recent improvement in e-commerce. In this chapter, the researcher has attempted to focuses specifically on the early history and evolution of the internet, e-commerce at the international level, and highlight basic features of e-commerce in general. Further in this chapter, the researcher dealt with the development of e-commerce and some issues in brief related to consumer protection. The chapter comprises of the following components viz. demographic profile, web and internet usage, purchasing habits and web versatility. Each parameter has been analyzed extensively and the results have been presented in the form of tables, figures and charts wherever necessary. The chapter deals with e-commerce in general, what is e-commerce, the advantage and disadvantage of e-commerce to the buyer and traders as well as studying the different kinds of e-commerce and popular online shopping platform like Amazon, Flipkart, e-bay, etc.

The third chapter titled *'Consumer Protection and Issue in E-Commerce'* focuses on analyzing the perceptions of the consumers towards digital buying. E-commerce has changed the way of living; it has changed the character of consumers and now consumers are named e-consumer. This chapter has tackled issues relating to consumers in the digital economy because e-commerce transaction is not bound by time and place so there are lots of issues relating to consumer security, privacy, and data protection, which have been covered in this chapter. For a better understanding of the issues pertaining to consumers, the researcher has divided them into two segments i.e. cyber tort and cyber crime. Privacy, negligence and defamation are major cyber tortuous issues in e-commerce. Nowadays increasing cases of cyber crimes are growing fast, such as hacking, phishing, fake links, social media issue, hacking bank accounts, etc. So the researcher has chosen to discuss the above mentioned issues in this chapter. The digital money Cryptocurrency and new WhatsApp terms and conditions 2021 and their impact on users are also discussed in this chapter.

‘*International Framework of E-Commerce’* is the title of **chapter four**. The chapter is divided into two parts, the first part dealt with the Information and Communication Technique (ICT). As per the study, it needed to discuss ICT because development in ICT tools at International levels like broadband, smartphone, digital devices and artificial inelegancy (AI), gave a new dimension to the e-commerce industry as well as consumer facilitation. The second part of this chapter dealt with the international legal framework, some of the international conventions like UN Model law on e-commerce, WTO rules, EU directives, OECD rules and the Hague convention have been discussed to understand the development of international law as applied in for the protection of e-commerce. In this chapter, the researcher concluded that technological changes bring challenges to the basic principles of business and have changed human life and property also. As far as India is concerned, there is no legislation which explicitly refers to the e-commerce dispute. The law is yet to be developed, especially in developing nations such as India unlike developed economies such as the USA.

Chapter five of the thesis titled the *‘Indian legal framework of E-Commerce’* is related to the law and policies of India. In this chapter, the researcher studied and analyzed different laws like the IT Act, Penal Laws, Evidence Act, etc., as well as a broad evaluation of the newly enacted Consumer Protection Act, 2019 in regards to e-consumer. In this chapter, the research study has mentioned that the law of e-commerce is a new phenomenon in India and people are not much aware of the online transaction so they need consumer awareness first.

The sixth chapter of the thesis titled *‘Internet Jurisdiction Issue and E-Commerce’* discusses the jurisdiction issue in e-commerce as one of the most important fact of international law because international law is based on states consensus and not based on universal acceptance. In this chapter, the research study has analyzed the nature of internet jurisdiction and why it needs clear law and policy at the international level. In this chapter USA, EU and Indian law on internet jurisdiction are analyzed and suggests a better environment for e-commerce law. The chapter also focused on the importance of the Hague Convention in detail because this convention is first on a choice of court agreement and accepted by many developed countries.

Chapter seven is the last chapter of the study. In this chapter, certain conclusions are drawn and some suggestions are also placed for consideration. Based on the findings of this research study, it is inferred that the problem of consumers in e-commerce needs to be addressed urgently. In India, there is no proper grievance mechanism for the victim of the online in the e-commerce market and thus is an area of primary concern in India which needs considerable work in the best interest of the domestic e-consumer and e-commerce at large.

TABLE OF CONTENT

LIST OF CASES

1. *Ajay Mitra v. State o f Madhya Pradesh, AIR 2003 SC 1069.*
2. *Amway India Enterprises Pvt. Ltd. v. 1Mg Technologies Pvt. Ltd. & Anr., CS (OS) 410/2018*
3. *Arif Azim case*
4. *Avnish Bajaj v State (N.C.T.) of Delhi (2005) 3 Comp LJ 364 (Del)*
5. *Bishwanath Prasad v. Dwarka Prasad, AIR 1974 SC 117.*
6. *Calder v. Jones case Calder v. Jones, 465 U.S. at 784*
7. *Manish Kathuria V. Ritu Kohli Case*
8. *Delhi High Court direction to all online companies on 8 July 2019*
9. *D'zine Garage Pvt. Ltd. rep. by its Director Mr. Hari Sethuraman v D'zine Café FZE & D'zine Café FZE v D'zine Garage Pvt. Ltd. rep. by its Director Mr. Hari SethuramanNirav Navinbhai Shah & 4 ors. v State of Gujarat, 2008 (36) PTC 614 Mad*
10. *Fatima Riswana v. State Rep. by ACP, Chennai & Ors AIR 2005 712.*
11. *Harrison v. Microfinancial Inc, 2005 US Dist Lexis 2804 (D. Mass., Feb. 24, 2005)*
12. *India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc & Ors 2007(35) PTC 177 (Del.)*
13. *International Shoe v. Washington, the Court66 S. Ct. 154 (1945)*
14. *Calder v. Jones, 456 US 783 (1984)*
15. *LICRA c. Yaho Scottish Daily Record (Apr. 13. 2000) 41.2000 WL 17093040o,*
16. *Mahadeo Prasad v. State of Bengal, AIR 1954 SC 724*
17. *Nasscom vs. Ajay Sood & Others, 119(2005) DLT 596*
18. *Shreya Singhal v. Union of India, AIR 2015SC 1523*
19. *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, Suit No.*

1279/2001 Delhi HC

20. *Syed Asifuddin and Ors. v The State of Andhra Pradesh And Anr. 2005 Cri LJ 4314*

21. *The Arzika case*

22. *WH Martin Ltd v. Feldbinder Spezialfahzeugwerke GmbH [1998] ILPr 794*

23. *World Wide Volkswagen Corporation vs. Woodson444 US 286: 100 S. Ct. 559 (US Supreme Court, 1980)*

24. *Zippo Manufacturing Company v. Zippo Dot Com, 952 F. Supp. 1119, 1124 (W.D. Pa.1997)*

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
ABA	American Bar Association
Ads.	Advertisements
ARPANET	Advanced Research Projects Agency Network
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
BCG	Boston Consulting Group
C2C	Consumer to Consumer
CBI	Central Bureau of Investigation
BHIM	Bharat Interface for Money
CAGR	Combined Annual Growth Rate
CBDC	Central Bank Digital Currency
CD	Compact Discs
CII	Confederation of Indian Industry
COD	Cash on Delivery
COVID-19	Corona Virus Disease 2019
DARPA	Defense Advanced Research Projects Agency
DCC	Digital Consumer Courts
E-Business	Electronic Business
E-Buyers	Electronic Buyers
E-Buying	Electronic Buying
ECF	Electronic Case Filing
E-Com	Electronic Commerce
E-cash	Electronic cash
E-Commerce	Electronic Commerce
E-Consumer	Electronic Consumer
E-Customer	Electronic Customer
Ed.	Edition
Eds.	Editions

EDI	Electronic Data Interchange
E-mail	Electronic Mail
E-exchanges	Electronic Exchanges
E-mail	Electronic Mail
E-Market	Electronic Market
eMarketer	Electronic Marketer
eProcurement	Electronic Procurement
E-Purchase	Electronic Purchase
E-Purchasing	Electronic Purchasing
E-Retailing	Electronic Retailing
E-Seller	Electronic Sellers
E-Selling	Electronic Selling
E-Service	Electronic Service
E-Shop	Electronic Shop
E-Shopping	Electronic Shopping
E-Store	Electronic Store
E-tail	Electronic Retail
E-tailing	Electronic Retailing
GDP	Gross Domestic Product
GUIDEC	General Usage for International Digitally Ensured Commerce
IAMAI	Internet and Mobile Association of India
IC	Informational Content
ICC	International Chamber of Commerce
ICT	Information and Communication Technology
IP	Interface Properties
IS	Information Systems
ISP	Internet Service Provider
M-Commerce	Mobile Commerce
MNC	Multi National Corporation
M-Shopper	Mobile Shopper
NSFNET	The National Science Foundation (NSF) Network
OTT	Over the Top
PC	Personal Computer

Pvt.	Private
RBI	Reserve Bank of India
SMEs	Small and medium-sized enterprises
UNSDGs	UN's Sustainable Development Goals
UPI	Unified Payments Interface
Tech.	Technology
TV	Television
UK	United Kingdom
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNGCP	United Nations Guidelines for Consumer
US	United States
USD	United States Dollar
VCD	Video Compact Discs
Vol.	Volume
WB	World Bank
WCRD	World Consumer Rights Day
WHO	World Health Orgainsation
WITSA	World Information Technology and Services Alliance
WTO	World Trade Organisation
WWW	World Wide Web

CHAPTER-1

INTRODUCTION

CHAPTER-1

INTRODUCTION

1. Introduction

It is hard to fail, but it is worse never to have tried to succeed.
In this life, we get nothing save by effort.

—Theodore Roosevelt

The Internet has dramatically changed the way we do business, whether it's finding new sources of revenue, acquiring new customers, or managing a business. E-commerce is common: it allows businesses to sell products and services to consumers globally. Therefore, e-commerce is the platform on which new methods of selling and distributing innovative products and services are tested electronically.

The Internet has reduced the world and brought it to the screen of a computer. The way we live has changed. There is a lot of information on the internet, which is available to anyone who can access it at any time and from anywhere. Simply by typing only a single word on a search engine like Google, you can have more information than can be handled. It is the cheapest, most rapid and efficient way for communication, commerce, entertainment and much more.

The internet opens up a completely new market for goods and services. It creates opportunities for a multifaceted arena that offers new efficiencies for sales, marketing, customer support, shipments monitoring, inventory monitoring and many other aspects of the total business model.

The choice has always been the holy grail for consumers. Today's consumers have a wide range of commercial options: traditional businesses, mega-discount stores, catalogues or direct mail from the market and the web.

The internet as a whole is a powerful medium in which consumers browse, research, compare and then buy online or, after having seen the ‘showcase’ online, would then buy online.

A great utility of the internet is that it brings the global markets to your door step through your smart phone. The consumer can sit in the comfort of his home while shopping around the world, looking for the best products at the best possible price. All these websites and information related to the products have been made available to the public by various people, governments, corporations, and organizations, etc., who wish to be visible and known.

At the beginning of the second millennium, we are prepared for one of the most important changes in our lives: the change to an internet-based society. Almost everything is changing dynamically at home, at school, at work, in government, even in our leisure activities. Some changes are already evident throughout the world. Others are just beginning. A very significant change is in the way we conduct digital business, 24/7 open table for a chat, discussing or sharing anything, anytime anywhere, really internet changed the universe of life, especially in the way we manage the market and shopping. This fact shows the importance of the term ‘electronic commerce’.

Electronic commerce or e-commerce describes how transactions are carried out through networks, mainly the internet. Today the internet is becoming an integral part of human life, it is like virtual food which gives one freshness when one wakes up in the morning. The shopping experience of online shoppers has changed, as virtual stores get convenience, variety and price scores.

The number of internet users has more than doubled since the year 2015, and now in 2020, it is available to 4,574,150,134 billion (58.7%) worldwide as of December 2019. Indian consumers are rapidly advancing towards adopting the technology. While the overall tele-density is.81.8%, the mobile tele-density is also high at 87% and 451 million people as of March 2019[1]. Additionally, during the same time, India beat the United States of America to become. the 2nd largest market after China.

In other words, electronic commerce has triggered a new revolution, which is changing the way one buys and sells products and services. It has affected a significant part of the world, including business, professions and, people. Its impact is not just the creation of web-based corporations. E-commerce is a structure of a new creation of a virtual world where we always live, no time of day, no time of night. American Vice President Albert Gore Jr. put it thus:

> "*We are on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks Mill allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress.*"

Electronic commerce has been making great profits and has invaded all the effects of each circle in the Indian market. With the guarantees of openness and accommodation, it has given the occupants and the foundation something to improve. The Indian government is also dedicated to supporting digital transactions and trying to achieve 100% digital literacy in the nation. The government is introducing a new digital payment policy and online policy daily, the government is focusing focus to make India a digital India and place the country in the world as a global leader.

The demonetization caused a greater reception of the benefits of Unified Payment Interface (UPI) mobile wallets which gave a catalyst to the medium of exchange without cash. The demonetization opened a new economic door for the consumers in metropolitan areas. The pattern of e-wallets became famous

---

[1]India has second largest population of monthly active internet users report *available* at https://www.livemint.com/technology/tech-news/india-has-second-largest-population-of-monthly-active-internet-users-report-1569500591581.html (last visited on March 03, 2020)

among consumers in urban India and also affected the rural area consumers. The underlying effect of demonetization has given the impetus required by the online payment system. When the impacts of the monetary crisis disappeared and circumstances were balanced, a considerable segment of the population reused the money again as the preferred exchange method for some time but today Unified Payment Interface is much more preferable among the consumers because it offers an attractive price, with greater choice and without the restriction of time. Nevertheless, the government had to do a lot of reform in online shopping because the consumer belonging to the rural areas and elderly people were worried to use e-wallets as a payment option.

Recently, world consumer day was celebrated by the United Nations on March 15. ‘The Sustainable Consumer’ was the theme of World Consumer Rights Day 2020, which talks about the global need for sustainable consumption and highlights the purpose of consumer rights and their protection in digital arena. The main aim of sustainable consumption is to accelerate to stimulate the effective use of resources. The emphasis needs to be on fair trade to reduce poverty and enable people of different backgrounds to lead healthy and safe lives. Sustainability is a difficult choice when consumers need to recognize their good buy. The World Consumer Rights Day 2020 is very important at the point of digital business methods. Internet has opened all business doors for every consumer of the world. E–commerce is without any limit, without any restriction digital exercise of all digital resources.

In 1983, the first consumer day was celebrated, which is an annual global affair. The consumer day takes place on March 15 on the occasion of the definition of consumer rights outlined by the President of the United States John F. Kennedy. He was the first global leader to formulate a vision of consumer rights and also apprehended the importance of consumers as a group. The date marks John F. Kennedy’s speech on the Consumer Law Act of 1962.

Consumer rights are part of a person’s fundamental rights because they protect him from corporate misconduct and the sale of fake products, it strengthens the common man to fight for his consumer rights, to fight the fake promises of companies that sell their products and, above all, consumer rights work as legal protection against corporate inequalities.

In the late 1950s and early 1960s, product marketing topped in the United States. Millions of American families have been fascinated by attractive product advertisements that have surrounded TVs throughout the day. The UN guidelines on consumer rights ensure certain legal rights to protect the consumer against frequent corporate abuse. The original consumer rights law included 4 basic consumer rights, but after the United Nations amendments in 1985, four new rights were added. The current bill includes eight basic consumer rights, which are essential rights to control the hegemony of the free market:

- The protection of the consumer from injury besides for vehicles, to assure that no products or services do not harm the consumer.
- The law asserts that companies should provide proper information to customers regarding their products and services; Disclaimer as legal information must not be misleading or inadequate.
- The consumer should have the right to like freely between products and the government should guarantee public competition so that consumers can choose from an ample variety of choices.
- The right to complain about product-related issues and companies should ensure those customer problems are dealt with honestly.
- The right ensures that consumers must have access to basic services to live a dignified life.
- The right allows consumers to remedy their complaints and to ask for an honest solution in the event of financial damage to the consumer.
- The right to consumer education emphasizes the role of consumers and governments in educating the consumer and in acquiring the knowledge necessary to make the appropriate decisions on the use of the product and to differentiate the choices available in the brand.
- This right preserves the sustainable use of each resource. The right of each citizen to live and act in a clean and secure environment and assure

that future generations also have access to a clean and secure atmosphere.

However, all the UN resolutions are only recommendatory in nature and thus not binding on states. This reason law and consumers, both are facing big challenges and issues between nations. However, the 1990s led to the liberalization of the Internet and, therefore, the privatization of the Internet. It is this privatization that establishes the current dynamics of the new system between e-commerce and e-consumer. E-commerce law was initially developed in order to provide consumer protection from online hackers. As we all know that e-commerce is a cross-border transaction and without limitation of time and place, thus the integral question is that how can the law protect consumers in case of online fraud or cyber crime.

E-commerce faces one significant problem that is an issue of jurisdiction. When parties to a transaction are from different countries and if any dispute arises between them, which law will prevail? The United Nations has adopted a Model Law on e-commerce and also the European Union has a law on e-commerce but all laws are insufficient to consider the issues of e-commerce. Each country being a sovereign power has its law and policy, no country is likely to enforce foreign court decisions.

In the context of information technology and e-commerce, amongst developing countries, India is like a beacon on the horizon of the new digital age. Its success is no more one-off or marginal in growth or sustainability. The story of India in this new economy is therefore of interest to policy-makers and managers across the globe and relevant for other developing countries. E-commerce has greatly affected shopping and generally the way people purchase goods and services. Today a consumer has millions of options to purchase anything. This situation puts much confusion on the consumer to buy because e-commerce websites offer him a great choice and cheap products. E-commerce has changed the consumer to e-consumer and the word ‘e’ expresses many facilities on one hand and a lot of risks another hand. So the risk associated with the internet is a big challenge at the global label. Today, the law is facing a lot of issues and is found incapable to consider all issues pertaining to e-commerce.

Electronic Commerce is a new and still emerging phenomenon and yet a fairly comprehensive body of literature, both in hard copy (books, journals, etc.) and in digital format on the Internet, it has changed the way of the use of the Internet and the world of shopping. As the importance of e-commerce has grown a large body of literature on it has appeared but mainly from the business or commercial perspective. There is no work available specifically on the law, policy, and administration of e-commerce with reference to consumer protection. No literature provides details about e-consumers issues and legal protection. The studies conclude that electronic commerce is growing in importance and detail discussions on the issue of consumer protection.

There is a need to encourage organizations and shippers to make advanced deliveries as the preferred exchange method. Another important aspect to remember is the security of the online transaction, as there is still much to do to ensure that the transactions are secured and secured with up to date administrative structures that can guarantee the Indian buyer that provides security from hackers.

1.1 COVID-19: E-commerce and Consumer

Be it the economic recessions or much-dreaded pandemic; the trend of the market is changing the entire course of businesses. With Covid-19, at its all-time high, the early signs of consumer behavior shifting can be palpable. While remote working is garnering much importance, the profitability of a majority of businesses, such as airlines and hospitality, are getting adversely impacted. However, this pandemic obviously has enough potential to change how consumers shop, consume information, and even towards how business works.

The world is facing a severe lockdown currently. With only a few people out on the roads, the number of those who have isolated themselves is increasing day-by-day. As a result, housebound consumers across the globe are turning towards online shopping, even for essential supplies. With lockdowns, brick-and-mortar stores i.e. traditional street-side businesses that offers products and services to its customers face-to-face in an office or store that the business owns or rents, are completely shut and badly hit. Brick-and-mortar businesses have found it difficult to compete with mostly web-based businesses like Amazon.com Inc., retailers are facing a harsh reality, considering that the government has enforced quarantine and restricted outdoor trips. With e-commerce, on the other hand, shipping and supply challenges are persisting.

The shopping habits and consumer behaviour is changing rapidly. To stay competitive, businesses have started to sell what's important presently. Some e-commerce sellers are adding soaps, sanitizer and other hygienic products to meet consumer demands.

The recent living standard of consumers is primarily stay at home and is turning the attention of people towards digital shopping and selling and virtual shopping that has become a leading and growing trend in the Covid-19 pandemic thereby adding more importance and success to the e-commerce business industry. Before the danger of the Corona Virus people were free to move and interact in all kinds of businesses and thus the domain of e-commerce business was not in consideration as it is nowadays. It can be understood in this way that the pandemic of COVID-19 resulted in either self-imposed or government imposed lockdown which is complete in some areas and partially imposed in others. People are hesitant to go back to their working places and resume the work from where they left it because the number of active Corona cases is increasing. The fear of getting sick is the primary reason behind the switching of people towards online shopping and this is the reason why the e-commerce market is rapidly making progress by leaps and bounds.

Covid-19 brings a lot of challenges for consumers. The online security and privacy violation are rapid, consumers are being trapped in many ways like online fraud, fake funds, UPI, fake call for demanding money for the victim of corona and help to poor people. This pandemic has created a new challenge before cybersecurity.

The year 2021, WhatsApp brought new privacy policy; users have to accept the new conditions. The terms will also have to be deleted if they are not considered. It is time till 15th May to think about whether to accept the conditions. More than 200 crore users worldwide use WhatsApp. Many questions related to these conditions will be coming to mind. New terms and privacy policies have been updated on WhatsApp. It says that users will have to agree to these policies. It is coming into effect from 15th, 2021. After this date, it will be necessary to agree. If you do not agree, you will not be able to use the account. You can visit the help centre for this. The policy is now getting the option of agree or not agree. The new policy is a danger for the users and they give the right to access users' data. Nowadays e-commerce modes are operating by social media with a new term and condition regarding users' privacy. Social media is a powerful tool for e-commerce platforms. The ability to not only direct shoppers toward a new product or an attractive deal, but to engage with them and create a sense of community, is incredibly useful. A complete social media presence also includes direct sales through some networks, as well as having the back-end tools in place to let customers share products and recent purchases with friends and followers through just a single click. But the harmful effect of social media is the possibility of the company and consumer network being exposed to cyber threats such as malware. Cyber hackers can install malware through social media platforms which is be very unsafe for consumers and potentially damage consumer privacy, financial loss, computer networks or computers.

The rise of digital wallets is making way for more convenient and instant payment systems, and as a result, it is changing the way of conduct business and consumers' tendency. The invention of cryptocurrency has changed the currency flow system for merchants and consumers. NO credit card, no debit card or UPI id, now all are the traditional mode of payment. cryptocurrency is going to replace all traditional payment systems.

It would be fair to assume that cryptocurrency and e-commerce have the potential to complement each other quite nicely – and, in a few cases, they already are. Cryptocurrencies, particularly Bitcoin, are already infiltrating the e-commerce industry, offering an innovative, viable and streamlined digital solution for many existing blockers. With the ability to appease consumer demand for immediacy and security, while expanding market share for retailers, cryptocurrencies could prove extremely beneficial for the e-commerce industry if adopted efficiently. More and more companies have grown to understand these benefits, leading to a surge in consumer attention, and it may not be long before we start to see the commercial use of cryptocurrency as a standard.

1.2 Need for the Present Study

Current electronic commerce is becoming popular in an emerging economy. Electronic commerce began in 1995. It requires digital goods to carry out their transactions. Digital goods are goods that can be delivered through a digital network. Electronic commerce is rapidly transforming the way companies interact with each other, as well as with consumers and governments. As a result of changes in the ICT landscape, electronic commerce is now growing rapidly in several emerging markets and developing economies.

Despite that, electronic commerce is a growing phenomenon; its future development is, to a large extent, hampered by the lack of appropriate payment systems. Since most of the e-commerce payments over the Internet are performed currently via credit cards and mobile wallets, an admittedly problematic payment medium due to costs, security and trust problems, the need for new secure transaction systems emerges from the existing circumstances.

India in recent years has achieved significant success in developing a domestic internet infrastructure and e-commerce sector and has emerged as a major destination for international business, especially related to information and communication technologies. Along with this growth, e-commerce dispute becomes more common in India too.

One of the most challenging and significant problem with e-commerce is security measures. Internet security is of immense importance to promote electronic commerce. Companies and other business organizations that keep confidential information on their websites should ensure that they have security measures to protect their websites from any unauthorized intrusion. The company could face security threats both externally and internally. Externally, the company could face problems of hackers, viruses, and trojans. Internally, the company must guarantee security against its technical personnel and its employees. Security can be maintained through the use of various security tools such as encryption, firewalls, access codes /passwords, virus scans, and biometrics. For example, a company could restrict access to the content of their website only by using a password or login code. Similarly, confidential information on websites could be protected by firewalls that prevent any form of external intrusion. In addition to the appropriate security measures, appropriate legal documentation would also be needed. For example, a company could have an adequate security policy that binds all the people who work in and with the business.

Violation of privacy and data protection is a second important concern in e-commerce. An important consideration for each e-commerce website is to maintain the privacy of its users. The use of innovative technologies and the lack of secure systems facilitate the collection of personal and confidential information about individuals and organizations. In July 2001, a dozen privacy groups filed a complaint in the United States about privacy issues in Microsoft's Windows XP operating system. Some features of the operating system store personal information, such as passwords and credit card data, so that users do not have to constantly re-enter this information while browsing websites. However, although the Operating System was successfully launched on October 25, 2001, privacy groups have still criticized the Federal Trade Commission for not taking any action on the complaint. There is no mechanism to stop online violence of privacy of the consumer because it is very difficult to trace and catch cyber criminals, recently in the 2017 *Ransomware* virus circulated overall network that seized to computer and laptop to use.

The jurisdiction in cyber space is a major concern on this point that e-commerce is an international transaction so this may determine will determine the scope of any liability that may arise against the website. Under the traditional rules of private international law, the jurisdiction of a nation only extends to people who are within the country or to transactions and events that occur within the natural borders of the nation. So there is a need to study to analyze all the above-mentioned problems and provide, suggest and feedback.

1.3 Review of literature

To probe the problem at hand in an efficient and effective manner, a review of existing and related literature is very important. As per the statement of Walter R., Borg, '*literature in any field forms the basis on which all future work will be built*'. If the researcher fails to build this foundation of knowledge provided by the review of literature, work is likely to be shallow and will often merely duplicate work that has previously been done better by someone other. Therefore, the review of the literature justifies the study, examines repetitive research work on the same subject, eliminates the risk of academic piracy and gives the researchers an understanding of what still remains to be done in the area of the subject under the study. Therefore, keeping in view the importance of the review of related literature, researcher attempts here to review the available literature on the subject under study. A brief review of related literature on the present study is given below:

Although there are not enough important books and articles written directly on the subject of the thesis, good work related to the subject was reviewed. The review of some of the books and articles, through which the researcher has passed, is as follows:

a) *Electronic Commerce Security, Risk Management and Control*: Marilyn Greenstein and Todd M Feinmam, Tata Mcgraw-Hill Copmany Limited, New Delhi 2000. This book provides students with the knowledge and better understanding of electronic commerce from a security risk management and control perspective. The e-commerce arena has grown rapidly in recent years. Large companies and even small businesses use e-commerce as a distribution channel. Companies like Amazon.com Flipkart.com are part of a growing segment of businesses that use e-commerce as the only way to do digital transactions with consumers. This book analysis all the security issue related to e-commerce and provides to the student to understand consumer behaviour in the online market. The big lacuna of this book is that it does not emphasis much on the legal aspect of e-commerce and consumer privacy in the virtual world.

b) *Legal Dimensions of Cyberspace*: edited By S.K. Verma And Raman Mittal, Indian Law Institute, New Delhi, 2004. This book is the first book in the country wherein every chapter has been written by the most experienced experts available in the country. This book is also intended to form the basis of an e-learning course on the subjects to benefit users all around the country. the researcher found this book very use full for all concerned with Internet/cyber transmissions and other information. However, there is no chapter directly dealing with the issue of consumer protection in e-commerce and also not provide legal analysis at the point of data protection.

c) *Internet Jurisdiction and Choice of Law in the EU, US and China:* written by Faye Fangfei Wang, United States OF America of Cambridge University Press, New York. This book is good on this point in that it provides detailed discussion regarding jurisdiction issues in cyber spaces.

This book also focused on solutions of obstacles and approach, examine the existing jurisdiction and choice of law, rules and purposed the interpretation of those laws and rules. This book also discusses the need for the modernization and harmonization of private international law, compares the current legislative framework in the USA, EU and China and suggests a series of ways to remove the barriers to the determination of cyber jurisdiction and choice of law of the nation for cross border transaction. This book is also intended to form the basis of international law of jurisdiction course on the subjects to benefit users all around the country. This book has been particularly beneficial for the purpose of the research for the chapter related to Internet jurisdiction but this book is not useful for e-commerce issues and e-consumer protection.

d) *Introduction to the Internet Law & Policy*, written by Rodney D. Ryder's, Lexis Nexis Butterworths publication, 1st ed., 2007. The book is uniquely designed for courses on the Internet or Cyberlaw, E-Commerce, or Data Privacy Law. The book provides mainly chapters on the perspective on internet related legal issues, security concerns, trade secrets and privacy, digital signature, electronic governance, attribution, acknowledgment, and despatch of electronic records, secure electronic records, and secure regulation of certifying authorities, digital signature certificates, data protection, tele-communication regulations. This book was designed to offer a concise, current, and practical resource for understanding the legal environment of the Internet and electronic transactions.

e) *E-Commerce in India: Assessments and Strategies for the Developing World*, Alwyn Didar Singh 63, Lexis Nexis ButterWorths India 2008. In the present scenario India has emerged as an IT leader on the global digital scene and is providing digital infrastructure in many developing countries. This book bestows a framework for assessing the success of such strategies in economies and businesses and uses it to present the status of fourteen developing states economies. As a result of globalization and in many ways its main feature, e-commerce represents the spearhead of success in this digital age. E-commerce, however, is less about electronics and technology and more about strategy and management. The book is a pioneering study on the policy and strategy of e-commerce as it has evolved in India. In doing so, it determines that many of the developing countries (including India) still lack fully appropriate and fully assimilated policies and strategies that have limited their potential for success in the digital economy. The book serves as both a tool and a guide to strategic planning for policymakers, practitioners and managers seeking to understand the main issues surrounding e-commerce, from standards and capacity issues to legal and financial frameworks and tax and international trade issues that particularly impact on developing economies.

f) The article, *India: The Consumer Protection Act, 2019: An Overview,* written by Gaurang Kanth and Divjot Singh Bhatia available at mondaq.com gives a very good overview of the new Consumer Protection Act 2019. It analyzes the consumer issue in the digital environment but it does not include the data privacy law in regards to e-consumer.

g) The article, *Legal Issue in E-commerce* written by Aashist Shah and Praveen, Nishith Desai Associate, Mumbai, available at www. Nishith desai.com is a very good article that provides legal problems and security issues in e-commerce. It includes a detailed discussion on international norms relating to data protection, privacy law, authentication of websites. This article provides great insight into the legal aspect of e-commerce.

1.4 Significance of the Study

The present study can prove to be of great significance in developing a framework that may prove instrumental in resolving the e-commerce issues and consumer protection policy in online shopping. The study will open a new door for e-commerce in a different way. It can concern one of the issues, such as greater privacy, artificial intelligence (AI), robotic commerce and some technological development. The studies of this research attempted to be as realistic as possible. If the study succeeds in its goal then it could be proved to improve the whole system of e-commerce and can help improve the status of the present day e-consumer since the study has discussed a number of aspects important for the consumer relating to e-commerce and also provides valuable suggestions in this regard.

1.5 Statement of Problem

Internet is a boundary-less service that uses the website hosted in a particular country that can be accessed from any part of the world. Thus, compliance with the laws of the principal country as well as those countries where such e-commerce websites target audience and customers is of prime importance. In the new models of business in e-commerce, it is important to keep in mind consumer protection issues. There is no separate consumer protection law that is specific to regulate online transactions. The concept of privacy and data protection are not addressed in any Indian legislation. Internet frauds and cyber crimes are growing much faster than ever. Misleading advertising is a tool to disseminate wrong information to influence the buyer-seller transactions.

The legal framework for project e-commerce in India also includes compliance with other laws like contract law, Indian penal code, etc. Further, internet shopping in India also involves compliance with the banking and financial norms applicable in India. The present legal system in India is not conducive to the growth of e-commerce, thus, e-commerce dispute resolution is more appropriate for such purposes.

In India, many companies do not give warranty on those products which was purchased through e-commerce since the e-commerce company was not authorized to sell that company's product. However, the consumer may have no means of knowing the same or may be unaware of the authenticity of the website. They also constantly face the challenge of cyber offences such as hacking, which means hackers can deface websites and steal valuable data from systems or phishing, that is the making of e-mail messages referencing web pages that are replicas of existing sites to make users believe that they are authentic sites.

Cyber crime is a big issue in e-commerce transactions. Cyber crimes take several forms sabotage, revenge, vandalism theft, data diddling, credit card and ATM card fraud, counterfeiting, bank embezzlement and the theft of secret documents. Launching malware or virus is another form of cyber crime. Maximum internet consumers are cheated by cyber fraud. In e-commerce transactions very few consumers are aware of cyber fraud and others do not know about genuine websites, fake calls and operate computers and ATM, credit cards in safe mode.

The international legal framework of e-commerce is not equal in each region because each country has its own law and policy and such law is enforceable only in their territory. So if a consumer buys a product or services from a company that has a server or office in another country, what options does the consumer have in case of a defect in the product or services.

1.6 Objectives of Research Work

The objectives of the study are to evaluate the law and policies of e-commerce and suggest protection of the consumer in online shopping, to point out the lacunae in the law and policy and to suggest better law to plug-in the concerned lacuna. Given all the above facts, the following objectives of the present study are being framed:

1. To delineate the difference between traditional commerce and electronic commerce.
2. To spell out the legal framework of the regulation with major limitations of e-commerce.
3. To study the challenges before e-commerce posed by consumer protection issues.

4. To analyze the effects of e-commerce on consumer rights, and to provide plausible solutions in e-commerce issues.
5. To discuss legal and other related implementation issues in the area of e-commerce.

1.7 Hypothesis

1. The protection of consumer rights is a major concern in e-commerce.
2. There is a lack of a uniform standard for the quality of goods and services, security and the issue of privacy in e-commerce. Multiple financial, organizational, technological and managerial issues are not being addressed.
3. There is a lack of national and international government regulations and industry standards regarding e-commerce.
4. Advertising affects consumers' choices regarding what they buy and it is not legally addressed.

1.8 Research Methodology

The present study is based on the method of doctrinal, in addition to descriptive, exploratory, historical analytical research methods shall be applied per the need of prospective study. Where the things are introductory, the method to be applied is descriptive. Regarding the analysis of the legal provisions and judicial decisions, the method to be applied will be analytical.

The information shall be based on the analysis of a secondary source of data. The secondary data is available from various journals, the internet, government publications, earlier studies, media reports, and books. The research is descriptive and narrative information using a secondary source of data. Some primary sources of data like UN Model law, Indian Penal Code, IT Act, and international Conventions could also be used in accordance with the requirement of the study. The present study will encourage existing knowledge about the legal and social aspects of e-commerce and consumer protection.

The selected research methods have resulted in a comparative analysis whereby sources, dealing with e-commerce on the one hand and consumer protection, on the other hand, are compared to each other.

Concerning the characteristics of e-commerce and consumer issues, the extensive reference to the available literature is used. Examples of such materials are books on e-commerce, data privacy, cyber jurisdiction, international convention, and consumer rights.

1.9 Delimitations

For the purpose of this thesis, detailed technical requirements like Software, EDI, and virtual network on how e-commerce works over the world and IPR issues are beyond the scope of this research plan and therefore, these are being left out.

1.10 Scheme of the work

The Ph.D. thesis "**Legal Regulation of E-Commerce: A Study with Reference to Consumers' Right**" is divided into seven chapters. The **first chapter** is the "Introduction" to the research work. At the initial stage, the selected area of research work has been identified. After the identification of the research problem, a synopsis of research work and its basic structure were developed. The main objectives of the research study are stated in Para 1.6 in this chapter. A review of the literature is also stated in Para 1.3 in this chapter. Para 1.7 of the hypothesis is constructed in which four assumptions are made. On the basis of research observations, utilizing qualitative and quantitative research methodology, all assumptions have been proved. Further, the selection of the research problem, statement of the research problem, the significance of the research study, the scope of the research study are also briefly mentioned in this chapter.

The historical development of both e-commerce and consumer protection systems is convoluted and complex. The researcher does not intend to provide a detailed analysis of historical developments. However, the researcher felt it necessary to provide a broader context within which to frame the most relevant legal principles and structures of e-commerce law and the foundations that underpin it. For this reason, **chapter 2** 'E-Commerce: A Conceptual Analysis' gives a basic exposition of the history and concept of e-commerce as well as short discussions on the nature and functions of e-commerce and provides figures to show present e-commerce user data in order to inform a comparison regarding the fundamental characteristics of e-commerce and discussed recent improvement in e-commerce. In this chapter, the researcher has attempted to focuses specifically on the early history and evolution of the internet, e-commerce at the international level, and highlight basic features of e-commerce in general. Further in this chapter, the researcher dealt with the development of e-commerce and some issues in brief related to consumer protection. Chapter deals with e-commerce in general, what is e-commerce, the advantage and disadvantage of e-commerce to the buyer and traders as well as studying the different kinds of e-commerce and popular online shopping platforms such as Amazon, Flipkart, e-bay, etc.

Chapter third is 'Consumer Protection and Issue in E-Commerce'. E-commerce has changed the way of living, it has changed the character of the consumer, who is now called an e-consumer. This chapter has tackled issues relating to consumers in the digital economy because e-commerce transaction is not bound by time and place, thus there is a lot of issue pertaining to consumer security, privacy, and data protection, which have been covered in this chapter. The chapter deals in detail with consumer issues for better understanding of such challenges and that the researcher has divided consumer issues into two segments i.e. Cyber tort and Cyber crime. Privacy, negligence and defamation are major cyber tortuous issues in e-commerce. Nowadays increasing cases of crime by computer and digital resources are growing fast, a crime like hacking, phishing, fake links, social media issue, online robbery on a people bank account. So the researcher has chosen to discuss the above mentioned issue in this chapter and also strives to create awareness for an online transaction. The researcher has also discussed in this chapter the important role of the digital money Cryptocurrency in e-commerce and new WhatsApp terms and conditions 2021 and their impact on users.

'International Framework of E-Commerce' is the title of the **fourth chapter.** The chapter is divided into two parts, the first part dealt with Information and Communication Technique (ICT). As per the study, it needed to discuss ICT because development in ICT tools at International levels like broadband, smartphone, digital devices and artificial inelegancy (AI), has given a new dimension to the e-commerce industry as well as consumer facilitation. The second part of this chapter dealt with international legal framework, some of the international conventions like UN Model law on e-commerce, WTO rules, EU directives, OECD, U.S.A. and Hague Convention have been discussed in order to understand the development of international law as applied in for the protection of e-commerce. In this chapter, the researcher concluded that technological changes bring challenges to the basic principles of business and changed human life and property also. As far as India is concerned, there is no legislation which explicitly refers to the e-commerce disputes; the law is yet to be developed, unlike the USA.

Fifth chapter of the thesis is titled 'Indian legal framework of E-Commerce' is related to the law and policies of India. In this chapter, the researcher has analyzed different laws like the IT Act, Penal Legislations, Evidence Act, etc., as well as a broad evaluation of the newly enacted Consumer Protection Act, 2019 with regards to e-consumer. In the conclusion of this chapter, the research study has mentioned that the law of e-commerce is a new phenomenon in India and people are not much aware of the online transaction so they need consumer awareness first.

'Internet Jurisdiction Issue and E-Commerce' is the **sixth chapter** of the thesis. The jurisdiction issue in e-commerce is the most important fact of international law because international law is based on states conscious which may not be based on universal acceptance. In this chapter, the researcher described the nature of internet jurisdiction and why it needs a clear law and policy at the international level. In this chapter USA, EU and Indian law on internet jurisdiction are analyzed and suggested a better environment for e-commerce law. The chapter also focused on the important Hague Convention in detail because this convention is the first on the aspect of choice of court agreement and has been accepted by many developed countries.

In the **last chapter**, on the basis of this research study, certain conclusions are drawn and some suggestions are also placed for consideration. Based on the findings of this research study, it is inferred that the problem of consumers in e-commerce needs to be addressed urgently. In India, consumer protection in e-commerce is not addressed in any legislation. Hence related hypothesis has been proved. The study finds that e-commerce is a cross-border transactions and the quality of products, services and other relating things are not similar in all countries. The lack of a similar standard to products, quality, security and issue of privacy in e-commerce. Several financial, organizational, technological, and managerial issues are not being addressed therefore hypothesis related to them got proved. The lack of globally accepted law on e-commerce resulted in various territorial issues in case of any dispute between parties. If A has an office in Hong Kong and sells a product to B who lives in India and B sells that product to C who lives in Japan, if there is any dispute between them, which law will be applied? Hence the related hypothesis has been proved. The influence of advertisements on consumer choice is undeniable, and that is why the advertisement for the same must be fair and truthful. Misleading advertisements distort competition and, of course, consumer choice. Even after 30 years of enactment of the Consumer Protection Act, 1986 as amended 2019 and even after a paradigm shift from *caveat emptor* to *caveat venditor*, manufacturers and service providers from all sectors exploit Indian consumers. Implementation of law relating to a misleading advertisement is a big problem in e-commerce. There is no proper implementation authority and proper monitoring authority in India. So, the related hypothesis is proven.

1.11 Future scope of the research

This research attempts to embrace a wide spectrum of possible issues with consumer protection and e-commerce. Future research may focus on the further development and validation of the concept of consumer protection and e-commerce. For instance, a new civilization of consumer acceptance of e-commerce may be developed and validated to become a reliable tool for gauging user acceptance of electronic payment systems and similarly related technology. Future work can be concentrated on the validation of specific factors that can influence consumer acceptance. It can concern one of the issues, like privacy, artificial intelligence (AI), robotic commerce and some technological development. The studies of this research attempted to be as realistic as possible.

Of course, the most natural consequence of this research is to take the suggestions even further. They can be moreover validated, enhanced and substantiated in the context of actual use or in larger-scale experiments. It is interesting to see how e-commerce may give birth to new technology and new risks associated with the internet. It may become like a robot hacking crime, robot commerce. The research gives scope for future study on new aspects of e-commerce and consumer protection. The conclusion and suggestions part of the research will definitely help all such people who use the internet for any task. There are many suggestions given in regard to social media, law, and policy, e-payments protections. The suggestions would be very fruitful for every man of society. People can adopt the suggestions so that they can feel safe and save their hard-earned money, it may play a great role in online life.

CHAPTER-2

E-COMMERCE: A CONCEPTUAL ANALYSIS

CHAPTER - 2
E-COMMERCE: A CONCEPTUAL ANALYSIS

2.1 Introduction

In this chapter, the researcher undertakes an in-depth multidimensional conceptual analysis of e-commerce in terms of its meaning, scope, nature and forms. The researcher explores the history and aspects pertaining to the internet as a quintessential starting point for the conception of e-commerce. The researcher also undertakes the study of e-commerce and its myriad advantages and disadvantages as a crucial aspect in understanding and analysing as to why e-commerce has changed the way of doing business across the globe.

It is human desire to strive for the invention of livelihood, which then develops as a matter of habit for carrying out various activities for essential for sustenance of life. One such activity has been in the intermingling of technology with this drive to innovate sustenance and livelihood and is commonly known as electronic commerce (hereinafter referred as e-commerce). This commercial field has been called by several names such as e-commerce, digital commerce, electronic commerce and information economy.

In the early 1990s, the business and consumer world encountered a new channel for conducting trade and commerce, which was named e-commerce. Over the years e-commerce has evolved into an accepted and acknowledged way of conducting business. E-commerce is ever changing and growing, creating. Phenomenal results in terms of growth both from a business perspective as well as a customer perspective.. With many organisations and people labouring in the field of electronic commerce, it has become very clear that e-commerce.is here to stay and organisations and customers are trying to get the maximum benefit from it.

At present digital commerce is a milestone in the era of globalization and in many ways the leading feature of e-commerce is to represent the cutting edge innovation in a digital economy. E-commerce stands for electronic commerce and relates to trading in services and goods through a digital medium. Usually it functions through the internet and is available in the form of a website, which sells goods and services directly from the website using a shopping cart or shopping basket system and allows debit or credit card payments. It involves conducting business with the help of the electronic media, making use of information technology such as Electronic Data Interchange (EDI).[1] In simple words, e-commerce includes buying and selling of services and goods over the digital medium like computer or smartphone. Customers can purchase anything right from a car or a cake sitting comfortably in his room and gift it to someone sitting miles apart just by the click of a mouse. E-commerce is a 24/7 living platform where consumers can freely exercise liberty in buying and selling products and services.

2.2 Defining of E-Commerce

The term e-commerce consists of two elements, electronic mode of commerce. E-commerce essentially involves an online transaction. This transaction ranges from the act of placing an order online to it being delivered at the chosen address and financial transactions such as a movement of money between bank accounts. The term commerce signifies the sum of all related commercial activities of transfer of goods to make profits. Commerce is the whole system of an economy that facilitates a business environment. The system includes legal, economic, political, social, cultural and technological aspects it is a system that in operation for business in any country. Commerce today involves a complex system that companies wishing to maximize their profits by offering products and services to a market with low production costs. In recent years, traditional models of business have become obsolete and, in many cases, do not provide enough revenue for the company's owners or shareholders.

[1] E commerce and EDI, *available* at https://www.tutorialspoint.com/e_commerce/e_commerce_edi.htm (last visited January 20, 2017)

In historical times, the inception of commerce took its initiation with the advent of a standardized currency money which expedited a wider exchange of goods and services. The ancient Indian merchants travelled from village to village to collect, for example, cotton thread from the spinners or cotton cloth from the weavers and sold them in the village where they were in demand. The ancient merchants gained a profit by providing the goods acquired. Thereafter this business system was followed with other commodities as well such as grains, pulses, spices and other products. This acted as a conception point for larger trade and commerce in the country through trade routes.[2]

The old Indian trade was facilitated by the invention of a new method of exchange. Before the coins were used, the goods were swapped or exchanged under the barter system. But the coins proved highly advantageous since they could be easily transported from one place to another. As the use of coins increased, more and more traders arrived. However, the coins from this period were rough silver and copper coins with an engraved pattern on them. Trade was not limited to small areas. Goods bought in the Ganga valley were transported via Punjab to Takshasila (Taxila) or via the Vindhyas mountains to the port of Bhrigukachcha (Broach). From there, the ships took them to western Asia or to southern India.[3] However, the drastic change in the modern day international trading system is based on principles of free trade which is facilitated through bilateral and multilateral agreements.[4] A system of international commerce has encouraged to develop the world economy but in combination with bilateral and multilateral agreements. to achieve free trade. Both these phenomenon lie in different planes but still reflect on the transition and growth of commerce over centuries. Especially, over the past two decades, companies in almost all sectors of the global economy have benefited from

[2] *Available* at https://brainly.in/question/7422987(last visited on March 3, 2017)

[3] Trade and commerce in ancient India, *available* at http://www.importantindia.com/2910/trade-and-commerce-in-ancient-india/ (last visited on March 3, 2017)

[4] Angshuman Hazarika, E.Commerce*:* "Expectations and shortfall" 2 Christ University Law Journal 59- 78((2013)) ISSN 2278 – 4322/doi.org/ 10.12728/culj.3.0 (last visited on October 23, 2016).

technological advancements and especially by the merging of the two in the form of e-commerce.[5]

E-commerce is an emerging concept that explains the process of buying and selling or exchanging products, services, and information over computer networks, including the Internet.[6] For a better understanding of e-commerce, some definitions of e-commerce are discussed below:

Carol Cram[7] defines e-commerce with reference to the term commerce. She says "the term Commerce refers to all the activities in which a company or an individual engages to complete a transaction. When you use the Internet to engage in some or all of these activities, commerce becomes e-commerce. Therefore, one can define e-commerce as using the Internet to assist in the trading of goods and services."

According to the editor-in-chief of the International Journal of Electronic Commerce, Vladimir Zwass, 'Electronic commerce is sharing business information, maintaining business relationships and conducting business transactions by means of telecommunication networks'[8]. Thus, e-commerce is the use of electronic mode to engage in commercial activities. Businesses use e-commerce to buy and sell goods and services, to create greater corporate awareness and provide customer service.

Paul Timmers states that e-commerce can be defined loosely as 'doing business electronically. E-commerce, or better electronic business, includes electronic trading of physical goods and of intangibles such as information. It encompasses all the trading steps such as online marketing, ordering, payment, and support for delivery.[9]

---

[5]J. Christopher Westland & Theodore H.K Clark., Global *Electronic Commerce-Theory and Case Studies 1(*MIT Press, 2nd edn., 2000).

[6] Efraim Turban and Jae Lee, *et. al.*, *Electronic Commerce: A Managerial Perspective* 4 (Prentice Hall International, Inc. 2000).

[7] Cram M. Carol, *E-Commerce Concepts 2,* (Illustrated Series, Course Technology, 2001) .

[8] International Journal of Electronic Commerce by Vladimir Zwass , *available at:* https://books.google. co.in/ books? isbn=1591403561 (last visited on April 15, 2016).

[9] Paul Timmers, *Electronic Commerce- Strategies and Models for Business-to-Business Trading* 13 (John Wiley & Sons, Ltd., 1999) .

The World Trade Organization (WTO) Ministerial Declaration on E-commerce[10] defines e-commerce as, "The production, distribution, marketing, sales or delivery of goods and services by electronic means."

Kanilesh Bajaj and Debjani Naglj[11] suggest e-commerce as an electronic means of transferring information. They state that e-commerce helps conduct traditional commerce through new ways of transferring and processing information, which is the heart of any commercial activity. Information is transferred electronically from computer to computer. This has transformed the way organizations operate.

E-commerce, in simple words, is the commercial transaction of services in an electronic format. In general terms, e-commerce is a business methodology that addresses the needs of organizations, traders and consumers to reduce costs while improving the quality of goods and services and increasing the speed of service delivery.

Kalakota and Whinston [12]define e-commerce from these perspectives:

- From a communications perspective, e-commerce is the delivery of information/products/services or payments over telephone lines, computer networks or any other electronic means.
- From a business process perspective**,** e-commerce is the application of technology in the automation of business transactions and workflow.
- From a service perspective**,** e-commerce is a tool that addresses the desire of firms, consumers and management to cut service costs while improving the quality of goods and increasing the speed of service delivery.
- From an online perspective, e-commerce provides the capability of buying and selling products and information on the Internet and other online services.

---

[10] *Available* at: https://www.wto.org/english/thewto_e/minist_e/mc9_e/brief_ecom_e.html (last visited on April 12, 2016).

[11] Kamlesh K Bajaj. & Debjani Nag, *E-Commerce- The Cutting Edge of Business* 12 (Tata McGraw-Hill Publishing Company Limited, 2nd edn. 1999).

[12] Ravi Kalakota & Andrew B Whinston., *Electronic Commerce- A Manager's Guide, Addison* 3 (Wesley Longman, Inc., 1997).

The "digital economy" is a relatively new concept in policy-making replacing terms such as "the information economy" in the 1970s, "knowledge economy" and "e-economy" in the 1980s, "new economy" in the 1990s, or "network economy" and "Internet economy" in the 2000s. Though the terminology may have varied, there still is a general agreement on certain fundamental principles in this regard. The basic idea of the digital economy is that the manufacturing of products, services, lifelong learning and innovation is made possible by modern technology support, transmission and processing in the context of market globalization and sustainable development.[13]

2.3 The Distinctive Nature of E-commerce

One of the most important changes currently transpiring in the world of business and trade is the introduction of electronic commerce. The influence of electronic commerce on appropriation, business collaboration, online shopping and consumer services and delivery has impacted every organization. At present e-commerce is changing all forms of business, functional areas and their important duties, ranging from advertising to paying online bills. It has also altered the character of business competition with new online companies engaging in cutting edge technology and innovative business models, and a variety of e-commerce related goods and services mushrooming all across the globe. Therefore, e-commerce provides unique opportunities for companies to expand worldwide at a small cost, to increase market share, and to decrease costs.[14]

The simple meaning of the term commerce signifies trading of goods and services by the exchange of money, goods and services and where these activities have been undertaken is called a market. Market is an institution designed to facilitate the transfer of legal right and title of ownership in goods, services, and properties. In the history of commerce, commercial organizations

[13] Carmen Nadia **"**Integrating Digital Economy and Green Economy: Opportunities for Sustainable Development" *TERUM* volume 6, issue 1(February 2011).

[14] Prospects of E-commerce in Indian business, *available* at http://www.ijariie.com/AdminUploadPdf/PROSPECTS_OF_E_COMMERCE_IN_INDIAN_BUSINESS_CONTEXT_C_1173.pdf (last visited on April 05, 2020.)

can be found in all stages of development. To understand electronic commerce, it is essential to understand the basic principles of commerce.

The basic components of e-commerce are related to the fundamental components of commercial transactions.

The term e-commerce with all its agnate and related expressions includes types of activities known by different names, but all associated with the trade and business activities. Trade and commerce have made distribution and movement of potential goods from one part of the world to the rest much more efficient. Hence trading helps us get what we need at the right time and place and also helps us to improve our standard of living. Trade is the bridge that connects producers and consumers through retailers, wholesalers and other commercial entities. Consumers get information about the different types of products through advertising and sales. Producers are regularly informed about the dislike of consumers through market research. the growth of e-commerce industry and commercial drives the growth of commercial agencies such as banks, transportation, storage, and advertising. Trade increases national income and helps a country earn foreign currency through exports and collection of import duties. Trade stimulates international commerce and foreign exchange and helps secure faster economic growth in the country.[15]

The Gartner Group[16] signifies the nature of e-commerce as an evolving set of:

a) Home-grown or packaged software applications that link multiple enterprises or individual consumers to enterprises for the purpose of conducting business.
b) Business strategies aimed at optimizing relationships among enterprises and between individuals and enterprises through the use of information technologies.
c) Business processes (such as procurement or selling or order status checking or payment) that, by definition, cross boundaries and

[15]Currency Fluctuations: How they affect the Economy a*vailable* at https://www.investopedia.com /articles /forex/080613/effects-currency-fluctuations-economy.asp (last visited on June 19, 2021)
[16] Definition of E-commerce, *available at:* www.gaftner.com/ (last visited on April 15,2016).

d) Technologies and tools that enable these applications, strategies and processes to be implemented and realized.

The International Trade Administration[17] emphasis on the nature of e-commerce to include:

a) Any activity that utilizes some forms of electronic communication resources in inventory, exchange, advertisement, distribution and payment of goods and services;
b) All forms of commercial transactions based upon the transmission of digitalized data, including texts, sounds and visualized images; and
c) The commercial transactions of services in an electronic format.

According to European commission[18], e-commerce encompasses more than the purchase of goods online. It includes a disparate set of loosely defined behaviours, such as shopping, browsing the Internet for goods and services, gathering information about items to purchase completing the transaction.

- From a business process perspective, e-commerce is the application of technology to the .automation of business transactions and workflow.

- From a service perspective, e-commerce is a tool that addresses the desire of firms, consumers, and management to cut service costs while improving the quality of goods and increasing the speed of service delivery.

- From an online perspective, e-commerce provides the capability of buying and selling products and information on the internet and other online services.

[17] Compbell, A.J., *Ten Reasons Why Your Business Should Use Electronic Commerce* pp. 12-14.(Business America, 1998).
[18] *Available* at: www.ecommerce-europe.eu/- (last visited on April 15,2016).

Peter Cunningham[19] emphasized that the impact of e-business is felt on all business activities and states that it is the execution by electronic means of interactive, inter-organizational processes. Here "electronic" is a combination of telecommunications and computing capabilities. He is of the view that e-commerce is an integration of business processes and IT.[20] According to him, the boundaries of electronic business are expanding all the time. Business encompasses the execution of interactive, inter-business processes.

According to the Internet Tax Freedom Act (ITFA), 1998[21], the ambit of e-commerce includes "any transaction conducted over the internet or through internet access, comprising of the sale, lease, license, offer or delivery of property, goods, services or information, whether or not for consideration."

On the basis of the above stated aspects of e-commerce its nature can be understood to signify a generic term that explains the electronic mode of doing business with or without the help of the internet.[22] So, the scope of e-commerce is a lot more than the use of electronic devices such as computers, internet, software, etc. In fact, this is a part of how one runs a company. The definition that is likely to be acceptable by people involved in electronic commerce by referring to its characteristics and nature can be as followed: The use of electronic communication resources like telex, facsimile, electronic mails, telephone, computer, EDI, EFT, etc and particularly the internet and its enabling technologies to engage in the exchange, buying and selling of services and products requiring transportation, either physically or digitally from location to location, usually in lieu of money. In a very broad sense, the nature of electronic commerce also refers to the effects that the electronic exchange of commercial information can have on the institutions and processes that support

---

[19] Peter Cunningham and F Friedrich roschl, "Electronic Business Revolution'' *Springer* 15 (Verlag, 1999).

[20] *Ibid*

[21] Internet Tax Freedom Act, *available* at*:* https://www.fas.org/sgp/crs/misc/R43772.pdf (last visited on April 15,2016).

[22] In broader sense e-commerce is a concepts that covers all types of commercial and business transactions which are affected by electronic means whatsoever which, .includes Telephone, Telex, Facsimile, EDI, EFT, electronic mail, computers and Internet etc. But specifically it is with Internet because Internet is the.most potent way or technique to perform business or commercial activities electronically. It is therefore; E-commerce.and digital Commerce terms are used interchangeably.

and govern the commercial activities. These include organizational management, commercial negotiation and contracts, legal and regulatory framework and financial settlement arrangements among many others.[23]

Therefore, electronic commerce encompasses in its nature commercial transactions between individuals and commercial subjects, which takes place inside or through electronic networks. The significant factor remains that the nature of e-commerce transactions are those which are channelled through an electronic medium.[24]

In new business phenomena, electronic commerce facilitates and increases sales opportunities for the seller and at the same time it increases purchasing opportunities for the buyer. Businesses can use electronic commerce to identify new suppliers and business partners. Negotiating price and delivery terms are easier in electronic commerce because due to the internet it can help companies efficiently obtain competitive bid information. Another distinct feature of the nature of e-commerce is its capacity to increase the speed and accuracy with which businesses. can exchange information and that it reduces costs on both sides of transactions. Many companies are reducing their costs of handling sales inquiries, providing price quotes, and determining product availability by using electronic commerce in their sales support and order-taking processes[25] especially by the use of mobile devices.[26]

It is for these distinctive characteristics that in the present scenario, the popularity of electronic commerce is fast growing since it provides great opportunity for commerce and provides great convenience to the consumer. E-commerce has become a bulwark for business over the past few years, especially with increased technical awareness amongst the masses about the

---

[23] Sacher, Report (1997), OECD, p 20.

[24] *Available* at http://14.139.13.47:8080/jspui/bitstream/10603/113273/12/12_chapter%201.pdf (last visited on May 15,2017)

[25] Gary P. Schneider, *Electronic Commerce*, 18 (Cengage Learning Customer & Sales Support, 9th edn. 2011)

[26] M-commerce landscape in-2016 hyper local and growing fast, *available* at: http://venturebeat.com /2016/01/16/indias-m-commerce-landscape-in-2016-hyperlocal- and-growing-fast/(last visited on March 7,2017)

use of the internet. It provides for a simplified procedure and efficient mode of business.

Electronic commerce or digital commerce refers to a wide range of computer-based business activities for services and products. It also involves any kind of business transaction in which the parties communicate electronically rather than through physical appearance or direct physical contact. E-commerce is the method of electronic communications and digital information technology integrated in business transactions to transform, build, and redefine links for value creation between or among organizations, and between organizations and individuals.

Electronic commerce widens the range of services and goods available to consumers and increases the size of the producers' markets. Furthermore, items can be modelled and customised before purchase. Purchases may be made round the clock from anywhere. Certain services can be delivered online itself. It even provides an opportunity to purchasers to gain access to services and goods that were previously beyond their geographical or financial reach. The converse of this is also true, sellers gain access to the purchaser who was previously beyond their reach. E-commerce lowers entry barriers, expands existing markets and creates new shopping experience. [27] It helps sellers engage in retail for launching new products and services and to attract consumers through innovative ways such as through offers and gifts.[28] E-commerce has also made marketing easier, feasible and affordable with greater coverage and outreach like never before.

2.4 History of E-Commerce

It is not an easy task to trace the history of e-commerce since it has grown sporadically across several dimensions particularly through business transactions and consumer behavior. E-commerce is one of the most significant part of modern business and an innovative of intellectual property. E-

[27] *Id.* at 10.
[28] *Available* at: http://oaji.net/articles/2017/1174-1484826380.pdf (last visited on March15, 2020).

commerce plays an important role in organizing the marketplace and in turn encourages honest commercial competition.

2.5 Advent of Internet

Understanding the history of the Internet is vital to understanding what is happening today on the Internet.[29]

The origins of the internet lies in the fears of the Cold War. In the year of 1950 and early 1960s, there was a broad concern in the United States about the possibility of a nuclear dispute with the former USSR. The dramatic successes of the Soviet space programme also contributed to adding fuel to these pre-existing fears and the daunting threat to the USA of losing its technological supremacy. These and such similar other factors led to the formation of the Defence Advanced Research Projects Agency (hereinafter referred as DARPA) within the US Department of Defence with the objective of regaining its technological superiority.[30]

Throughout the 1960s the growth of technology to achieve data transfer between computers took place along with the acceptance of the concept of "ARPANET"[31] i.e. the computer network for DARPA. The preliminary data exchange between computers in the ARPANET in 1969 did start a new era in communication technology, but it was still not possible for networks of different architectural designs to communicate with one another as there was a lack of common language or 'protocol'. Attempts to develop such a protocol continued in the 1970s, mainly under the direction of Bob Kahn and Vint Cerf and, finally in 1983, the Transmission Control Protocol/Internet Protocol (TCP/IP) was developed as the industry standard. For the first time, different

[29] Jill Ellsworth H. & Matthew V.Ellsworth, *The New Internet Business Book*, 3 (John Wiley & Sons, Inc., 1996)

[30] https://books.google.com/books?id=xOdRcVIuyUwC /(last visited on March 7,2017)

[31] ARPANET, in full Advanced Research Projects Agency Network, experimental computer technology that was the forerunner of the Internet. The Advanced Research Projects Agency (ARPA), an arm of the U.S. Defence Department, funded the development of the Advanced Research Projects Agency Network (ARPANET) in the late 1960s. Its initial purpose was to link computers at Pentagon-funded research institutions over telephone lines.

computer networks could interact with one another and the 'Internet' (meaning inter-network communication) in the present day sense became a possibility.[32]

In the 1980s, the widespread growth of local area networks (hereinafter referred as LAN), PCs and workstations fuelled growth, and researchers and developers increased. In this way, the number of hosts (computers with registered IP addresses) that communicated with each other during this decade increased from approximately 200 to more than 300,000. In 1986, the United States founded the National Science Foundation (hereinafter referred as NSF) and the NSFNET[33], to improve internet access. This led to an explosion of internet connections mainly from universities. In 1990, ARPANET, the mother of the present internet was decommissioned and NSFNET continued the backbone network of the internet until 1995.[34]

The advent of the World Wide Web on the internet represents a turning point in e-commerce by providing an easy-to-use technological solution for information publishing and. dissemination.[35] The web made e-commerce a cheaper way of doing business (economies of scale) and enabled more diverse business activities (economies of scope). The web also allowed small businesses to compete on a fairer technological level with wealthy multinational companies. The other significant reforms included the development of search engines, web browsers and search engines which further brought the internet within the reach of almost anyone with a computer. By the year 2000, according to the US Internet Council, the web contained over two billion unique pages, 6.4 ran servers and 4.5 million sites.

In the year of 2000-2001, two major industry associations produced separate reports on e-commerce in India. The two reports were published in the same period, i.e. from June to July 2001. One was prepared by the National

---

[32] https://books.google.com/books?id=xOdRcVIuyUwC/(last visited on March 7,2017)

[33] The National Science Foundation Network (NSFNET) was a program created and funded by the National Science Foundation to coordinate and promote advanced research and education in networking in the United States. NSFNET served as a hub providing access to the five university based super computer centers created by NSF

[34] Internet World Statistic, *available at*: http://www.internetworldstats.com (last visited on March15, 2020).

[35] Ravi Kalakota & Andrew B. Whinston, *Electronic Commerce- A Manager's Guide*, 7(Addison-Wesley Longman, Inc., 1997)

Committee for Electronic Commerce created by the Confederation of Indian Industry (CII), while the other was sent by NASSCOM[36] and prepared by the Boston Consulting Group. Both reports were positive about the growth of e-commerce in India. The report of the Confederation of Indian Industry (CII) had estimated that the volume of electronic commerce will reach Rs 500 billion in 2003, of which B2B will be Rs 420 billion and B2C will be Rs 80 billion (CII, 2001). The NASSCOM-BCG Report, on the other hand, had estimates for the same year that the total volume of e-commerce will be Rs 1,950 billion, out of which Rs1,920 billion will be on record of B2B and Rs 3 billion will be on account of B2C (NASSCON and BCG,2001). E-commerce extension for the year 2001 was estimated to be Rs 150-200 billion according to NASSCOM and BCG, 2001 reports)[37].

In India, the e-commerce industry is expected to form the biggest part of the internet market with a value of nearly USD 100 Billion by 2020.[38] Internet Shopping is becoming increasingly popular and internet sales are estimated to grow from $172 billion in 2005 to $429 billion in 2015.[39] According to the worldwide statistics, there are 32 countries with more than 46.4 % of internet penetration rate.[40] The ability of internet users has also increased from 16% to 42%.[41] The internet has had a significant role in the changing consumer behaviour and market trends as well. It has contributed to the emergence of an era of consumer empowerment. In the digital economy, the consumer is the king of the market and has a plethora of choices available to him to choose from in the open market. In addition to transforming and revolutionising the retail sector in India, it is also promoting MSMEs to jump the evolution loop by implementing means of financing, technology and training. The advent of

---

[36] The National Association of Software and Services Companies (NASSCOM) is a trade association of Indian Information Technology (IT) and Business Process Outsourcing (BPO) industry. Established in 1988, NASSCOM is a non-profit organisation.

[37] An Analytical Study Of E-commerce Growth In Developing Country Like India, *available* at: www.isrj.net (last visited on September 20,2016)

[38] Ease of doing business, 2015, World Bank, *available* at http :// Indian express. com/ article/ business/economy/india-ranks-130-in-ease-of-doing-business-jumps-12-places-world-bank-report (last visited on September 18,2016).

[39] *Id.* at 34.

[40] *Id.* at 10.

[41] *Id.* at 13.

technology-enabled innovations like Hyper-local logistics, digital payment, analytics-driven customer engagement and digital advertisements have enabled e-commerce industry to develop at an exponential rate.[42]

Indian consumers are rapidly advancing towards adopting technology. While the overall tele-density is.81.8%, the mobile tele-density is also high at 87% 451 million people as of March 2019[43]. Additionally, during the same. time, India beat the United States of America to become. The 2nd largest market after China[44] for smartphones with over 220 Million users. This was attributable to the availability of highly affordable smart phones and with easy-to-use features which aided first-time smartphone users leapfrog from the desktop/laptop phase. Internet penetration is also significantly rising with the number of. Internet users at 354 Million as of September 2015.[45]

In addition, there is a shift in mobile usage from merely the voice function to data driven usage. Mobile internet spending has risen from 54% to.64% from 2014 to 2015. This is due to access and availability of high-speed 3G & 4G internet connectivity at affordable rates and has therefore resulted in a steep increase in the rise of transactions done via mobile[46].

Characteristic	Value in billion U.S. dollars
2021	84
2020	64
2018	50
2017	39
2025	188

Table 1. Size of e-commerce industry in India, The size of the Indian e-commerce market in 2014-2018 with projections to 2025.[47]

[42]India the sleeping dragon report on Indian e commerce 2017, *available* at: https://www.slideshare.net/ Anand BR1/ (last visited on September 18, 2016).

[43]India has second largest population of monthly active internet users report-https://www.livemint.com/technology/tech-news1569500591581.html (last visited on March3, 2020).

[44] India, the second largest smartphone market, *available at* http://www.counterpointresearch.com/india handsetmarket 2015 (last visited on September18, 2016).

[45] Mobile Internet in India 2015, by IAMAI and IMRB

[46] *Ibid*

[47] Market size of e-commerce industry across India from 2014 to 2018, with forecasts until 2027, *available* at https://www.statista.com/statistics/792047/india-e-commerce-market-size/ (last visited on June 19,2021)

The rise in the middle-class consumers and changing shopping habits has greatly contributed towards the significant spike in the shopping demography. Increased access to global products and services at a click of a button and the ease of doorstep delivery, including delivery to the remotest of locations has further driven up these number.

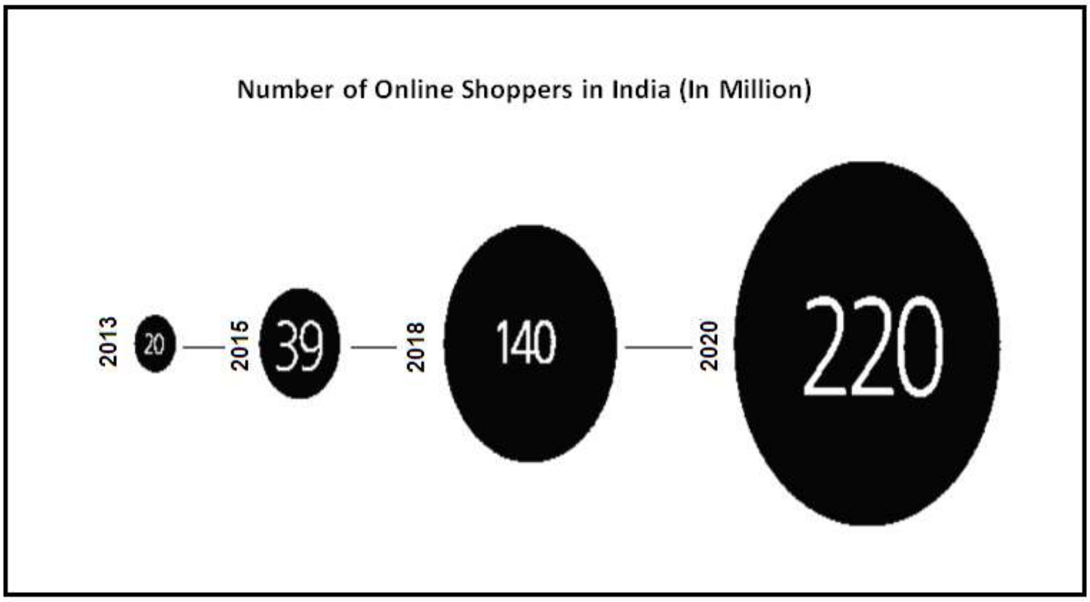


Figure 1. Number of online shoppers in India (includes only B2C e-tail excluding online travel and classifieds**)** Source – Euromonitor, IAMAI, Media reports Estimated Numbers.

Therefore, to indicate the milestones of the internet crucial to the development of e-commerce are as under:

1957	The Soviet Union launches Sputnik, the first artificial satellite.
1958	To counter Soviet technological advances, the U.S. forms the Advanced Research Projects Agency (ARPA), with the Department of Defence, to develop U.S. leadership in science and technology applicable to the military.
1969	US Department of Defence starts the first network among major research centres in the US. ARPANET, the forerunner of the Internet, established with four nodes: UCLA, Stanford, UC-Santa Barbara, and University of Utah.

1970:	First applications of electronic data interchange (EDI).
1971	15 major connections or nodes established. E-mail introduced.
1973	Defence Department started developing various forms of file transfer. First international connection to ARPANET, University College of London. Initial work on a transmission protocol (hereinafter referred as TCP/IP) that allows diverse computer networks to interconnect and communicate with each other.
1974	BBN opens Telnet, the first commercial version of ARPANET
1982	Transmission Control Protocol (TCP) and Internet Protocol (IP) established by ARPA. This leads to a definition of an "internet" as connected set of networks, specifically those using TCP/IP, and "internet" as connected TCP/IP internets.
1983	Internet Activities Board (IAB) is created.
1984	Domain Name Service (DNS) introduced.
1984	Science fiction author William Gibson was the first person who uses the term "cyberspace" in his novel, *Neuromancer*..Internet host computers (computers with registered IP address) exceed 1,000.
1986	US National Science Foundation created internet-based telephone lines.
1987	The number of hosts (computers on the Internet) reaches 10,000.
1988	The number of hosts on the Internet crossed 60,000. However, an internet worm disabled 6,000 of 60,000 internet hosts. A Cornell University graduate student created the worm. Infected computers were connected through ARPANET and other E-mail networks in the Internet loop. Some of the US's top science and research centers were affected.
1989	Over 100,000 hosts on the internet registered.
1991	The World Wide Web [WWW] created by CERN in Switzerland. Sir Tim Berners-Lee, working at CERN in Geneva,

develops a hypertext system to provide efficient information access. He posts the first computer code of the World Wide Web in a relatively innocuous newsgroup, “alt.hypertext”. Later, people refer to the internet itself as the Web.

1992: One million hosts on the internet.

1993: InterNIC created to handle Domain Name registration

1994: Pizza Hut sells pizza on its website. First Virtual, the first cyber bank, opens.

1995: A total of 6.6 million hosts or computers on the internet.

1996: An estimated 12.8 million hosts, 212,155 websites and 25 million users of the Web, about 90% of them in the US.

1997: 1.3 million domain names registered.

1997: 22 million servers, 40 million users on the WWW. Inception of business-to-business (B2B) e-commerce. US Postal Service issues electronic postal stamps.

2000: 110 million users and 72 million Domain Names.

2003: 802.2 million users and 233 million hosts.

2011: Internet users tally almost 2 billion. Users in over 200 countries stood connected.

2014: India has started Digital India programme.

2019: Presently there are 4,536,248,808 million users of internet in the world 58.8% of the world population[48].

Therefore, the abovementioned history of the internet can be divided into seven general stages of development[49]

1. The early years

2. Experimental networking

3. Discipline-specific research

4. General research networking

48 Internet world statistics

49 Rajesh Chakrabarti & Vikas Kardile, *The Asian Manager’s Handbook of E-Commerce*, 9 (Tata McGraw Hill, New Delhi, 2002).

5. Privatization and commercialization

6. National information infrastructure

7. High performance computing and communications

2.6 Key drivers of E-commerce

E-commerce drivers connect millions of buyers and sellers around the world and are significantly expanding business online. They create a chance for retailers throughout the world to increase the visibility of their products or services. E-commerce companies like Amazon.com, Alibaba.com, and Flipkart.com offer a platform for buyers and sellers to meet online. Traders have the opportunity to showcase their products, services and reach a large target audience and on the other hand buyers have the opportunity to browse through numerous products from various sellers, in different locations and compare prices, all on the related platform.[50]

E-commerce platform sales transactions are initiated when the two parties agree on a price for the product or service chosen using the payment methods available, with the e-commerce platform acting as a facilitator of the transactions. Once the payment has been received by the customer, it notifies the seller to send the goods to the buyer and the payment is transferred to the seller. Sometimes other services such as warehousing, logistics and customer service are provided to help sellers concentrate on growing their businesses.

2.6.1 Major E-commerce drivers

Curtesy the internet, now everyone can buy almost anything, at any time and from any location. Understanding the questions that concern consumers before purchasing online is a greatly pertinent for a key driver of e-commerce. It helps them understand the leading factors and establish the right e-commerce website for selling and buying products and services.[51] The following are some of the questions which concern consumers before purchasing online:

---

[50] E-commerce drivers , *available* at: https://www.slideshare.net/IraTobing/bringing-smes-onto-the-ecommerce-highway-english (last visited on April 7,2020)

[51] Major E-commerce drivers , *available* at www.whisbi.com (last visited on April 7,2020)

- Can I trust this website? Is it perfectly legal? Is it secure enough to do financial transactions on this website?
- How are the delivery and return policies of the website? How much time does it take for shipping the products? What happens if the product will not be what I anticipated? How will I refund products to the store (credit or replacement)? Who will pay for the shipping in case of return of the product or services?
- What is the conclusive price of the products including all additional costs? Is this the most reliable available deal?
- Is there enough information on the e-commerce website to make a purchase decision?
- Why am I actually purchasing this? Do I actually like it? What if I have some confusion and questions about the product?

Knowing the leading factors in successful e-commerce can help consumers and businesses to choose a better service and to get a clear idea of the right e-commerce website for financial transactions. Some of the most important drivers in e-commerce are:

Amazon :

Amazon is the largest e-commerce retailer in the US and operates 10 online markets (websites) worldwide, in Canada, China, France, Germany, India, Italy, Japan, in Spain, the United Kingdom, and the United States. Amazon allows companies to advertise their products and to pay for it to be listed as a top product. The order processing centers provide archiving and order fulfilment, including customer service and third-party vendor returns.

Alibaba:

Alibaba was founded in 1999 by former english teacher Jack Ma, who raised $ 80,000 from 80 investors to launch an online marketplace for Chinese companies. He became the richest man in China and his estimated net worth exceeded $ 47 billion. The company has acquired 4.5 million registered Indian users, accounting for the second highest paid user on the platform after China. Indian SMEs can also benefit from assistance in terms of funding, national and cross-border logistics, inspections and certifications, technology and business education for SMEs on this platform. In India, the Chinese Company has partnered with companies like ICICI Bank, Kotak Mahindra Bank, Crisil Rating, Tally, Capital Float, Jeena, SGS and Mypacco to help Indian SMEs grow their business. the largest online retailer Alibaba Group India is the second-largest market in the world.[52]

eBay:

eBay, the global online auction and selling company, was founded by Pierre Omidyar in 1995. eBay was one of the first companies to design and market a website that brought together buyers and sellers of goods and services. It provides for a multi-million dollar business with operations in more than 30 countries. e-bay as an e-commerce platform offers individuals and small businesses to expand in the online market space and provides for over a hundred million registered members around the globe. eBay started its business in India in 2005 and provided a solution to a long standing problem for Indian traders who were looking for a limited business opportunity. eBay has helped establish a negotiating platform that offers sales of products through auctions, quick buy, and classified modes of consumer-to-consumer trading.[53]

Mercado Libre:

MercadoLibre is Latin America’s leading e-commerce website. Headquartered in Argentina, it offers a cross border trade program for foreign sellers in Brazil and Mexico and will eventually be available across the Latin American coutries.

[52]History of alibaba, *available* at: https://www.thestreet.com/world/ -15145103 (last visited on April 20, 2020).
[53] Ebay india how did ebay enter india 2020, *available* at https://timesnext.com (last visited on April 8,2020)

Jumia:

Jumia, the leading e-commerce platform in Africa, was established in May 2012 in. Nigeria as a part of the Africa Internet Group (AIG). The company operates in Algeria, Cameroon, Côte d'Ivoire, Egypt, Ghana, Kenya, Morocco, Nigeria, Senegal, Uganda and United Republic of Tanzania.[54]

Souq:

Souq is the largest e-commerce platform in the Arab world, and currently delivers to Bahrain, Egypt, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates.

Flipkart:

Flipkart is one of the main Indian e-commerce website and is headquartered in Bengaluru, India. It was established in 2007 by co-founders Sachin Bansal and Binny Bansal. The company initially concentrated on selling books, before expanding to other product categories such as consumer electronics, fashion, household, and food items and lifestyle products.[55]

In March 2017, Flipkart had a 39.5% market share in the Indian e-commerce sector. Flipkart is largely dominant in clothing sales (a position that has been strengthened by its acquisitions of Myntra and Jabong.com). In August 2018, US based chain store Walmart acquired a 77% controlling stake in Flipkart for $ 16 billion, worth $ 20 billion.[56]

Snapdeal

Snapdeal is an Indian e-commerce company developed by Kunal Bahl and Rohit Bansal in February 2010. Its headquarters are situated in New Delhi. In 2014, Snapdeal had 3,000,000 sellers, over 3 million products (over 30

---

[54] Jumia african amazon , *available* at https://www.textmaster.com/blog/jumia-african-amazon/(last visited on April 8,2020)

[55] Flipkart , *available* at https://en.wikipedia.org/wiki/ (last visited on September 20,2019).

[56] *Available* at https://economictimes.indiatimes.com/news/company/corporate-trends/from-2bhk-to-8-3-lakh-sq-feet-the-flipkart-story-so-far/a-look-back/slideshow/64092726.cms(last visited on September 21, 2019)

million) in 800 categories, with more than 1,25,000 regional brands. Its services are available across domestic and international retailers and provides services to 4,000 cities across the country.

On 20 November 2019, International Trademark Association (INTA) registered Snapdeal as part of its endeavors to promote the protection of intellectual property on the digital marketplace. Snapdeal also manages a "Brand Register" program which allows sellers on Snapdeal to have their own registered trademarks, tradenames, etc. To obtain exclusive rights to sell your product in the relevant categories on the Snapdeal market over 1,000 brands are now part of its register.[57]

2.7 International nature of E-Commerce

In the era of globalization digital revolution has changed the business system. The seller-buyer, buyer-seller, manufacturer and buyer-seller relations all stand digitalised. The identity and the authentication of persons in the business transition are unknown and often do not have any direct interaction. The advent of the internet and internet compatible electronic devices, has enabled global access to the world of e-commerce allowing even small regional businesses to be instantly become an international business. When companies use the. web to improve their business process, they are automatically operating in a global environment set against the international phenomena of e-commerce. However, the issues faced are often common across all international e-commerce businesses which include trust,. culture, language, government, and infrastructure. These issues are discussed as follows:

2.7.1 Trust Issues on the internet

Trust plays a dynamic role in social and business relations. It functions as a powerful. tool in complex environments to reduce uncertainties and enable reliance on one and another. Trust constructs business, institutional and personal relationships and is particularly important in the global digital

[57] Snapdeal, *available* at https://en.wikipedia.org/wiki/Snapdeal(last visited on September 20,2019)

environment. The probability presented by the digital economy will not be realised in the absence of trust.

One highly probable issue concerning trust pertains to the privacy of the person and his information which is depicted in the data that over half of all online respondents in the study (57%) were sceptical about personal privacy information from e-commerce sites. Individuals from Mexico and Thailand (67%) accounted for the most concerned customers, followed by China (66%) Philippines (66%), Turkey (66%) and South Africa (65%).[58]

This aspect is crucial as it provides the foundation for the e-commerce platform to develop business relationships with their consumers. Businesses with established reliability in the physical world usually create trust by assuring that the consumers already know who they are. These businesses can rely on their established brand titles to create trust on the Web. New companies that want to organise online businesses face a more difficult challenge because a kind of invisibility exists for companies trying to establish a web presence. A now-famous cartoon in 1993 that appeared in The New Yorker magazine is shown in Figure 1. The figure exemplifies the inherent invisibility of the Web in a humorous way.

The cartoon depicts that there is no potential customer visiting the site since a customer cannot determine just how large or well established the company is simply by browsing through the web site's pages. Thus website visitors will not become consumers unless they trust the company behind the site. Therefore, planning is crucial for establishing credibility. Web sellers can't assume that consumers will believe that the site is faithfully managed. Therefore, it is a rational presumption that the consumer will think about inherent lack of trust in "strangers" on a digital platform, since till now such people have been used to doing business with known persons and not strangers. However, when over years a company grows to become a large corporation

[58] *Available* at: The Nielsen Global Connected Commerce Survey, January 2016 (last visited on September 21, 2019)

with multinational operations, its reputation grows adequately. Before a company can do business at a multinational level, it is necessary that the company demonstrates its credibility to its consumers over several years as it gets businesses through e-commerce. In the meantime, the company must constantly strive to find ways to overcome this well-founded tradition of distrusting strangers because for a company to truly grow globally, it has to constantly invest in its future and successfully create trust amongst existing consumers in order to attract more future consumers.[59]

Figure 2 This classic cartoon from The New Yorker illustrates anonymity on the Web.

2.7.2 Language Issues

Multinational companies realize that to effectively do their business in other cultures is to adapt to the cultures of such countries. The phrase "think globally, act locally" is often used to describe this approach. The first step that a web business commonly takes to reach potential customers in other countries is to provide local language versions of its website. This may mean translating the website into another language, more particularly into regional speech.

[59] *Available* at: https://books.google.com/books?id=Kx9UDt0SMy4C (last visited on April 21, 2020)

For instant, a typical website of a company in the European Union can display essentially the same pages in more than five languages. Contrary to this, in early 2001, there were only thirty-five Fortune 100 companies that had the website in several languages other than English. In 2001, nearly eighty-five percent of the entire websites were in English. However, only 45% of internet users spoke their native language, which is English. The percentage of native English speakers are decreasing day by day. If the e-commerce website can encourage more than one language, it will generate more benefits.[60]

A company can truly be global if it embraces the several spoken languages in the world. The website set up in multilingual languages helps to build trust and thus creates the foundations for a long-term relationship. However, translating the foreign language into plain English can be quite difficult; sometimes it can put the company at risk.[61] For example, Pepsi-Cola's motto "Come alive with the Pepsi Generation" translated into Chinese, unintentionally translated to "Pepsi brings your ancestors back from the dead".[62]

The biggest mistake that a company can assume is that everyone speaks English. This is pertinent since if the consumers find it difficult to understand the language of the website, the purchasing process would become too complex and would require too much effort and therefore may even lose interest in the company website.

Another instance of dilemma is the presumption that consumer should be aware of difference in a single language on the basis of dialect. For instance, the American gray spelling in Britain becomes grey, and the meaning of hood changes from the type of hat in the United States to the hood of a car in Britain. Another instance is the Chinese language which has two main writing systems: Simplified Chinese, which is used in mainland China, and Traditional Chinese,

---

[60] Multilingual issues in global e commerce websites, *available* at: https://sourceessay.com/multilingual-issues-in-global-e-commerce-web-sites/(last visited on May 10,2020)

[61] *Available* at: sk.sagepub.com 2019 (last visited on May 10,2020)

[62] *Ibid*

which is used in Hong Kong and Taiwan.[63]

If a company can introduce more than one language, it can be more profitable. These estimates have been justified to potentially increase the company's profits by three hundred percent. In 2003, the Forrester Research found that Japan and Europe had earned about half of their revenue from e-commerce sites. It can be seen through these websites that corporate consumers are more comfortable using their mother tongue on the website due to an associative sense of familiarity and therefore wish to continue browsing such websites.

So to give consumers a fulfilling experience and to give them a satisfying experience, it is advisable to offer them the best shopping experience and information in the language they are most comfortable in. Also, companies try to make sure that this information is presented in a very clear and easy to understand way and write everything in the language best known to the consumer of that nation. Even many languages require separate dialects and many translations. For example, Spanish languages have different dialects spoken in Mexico, Spain and Latin America. Therefore, it is important to check and translate the differences in spelling and the precise meaning of words. As the web company grows, it becomes more selective in its translation efforts.[64]

2.7.3 Cultural Issues

Another element of business confidence is the anticipation of how the other party will act in specific circumstances. The goodwill of a company expresses its expectations of how it will behave so that companies with established brands can develop an online business faster and easier than a new business with no reputation. For example, a potential buyer may want to know how the seller will react to the buyer's allegations that the seller has misrepresented the quality of the products sold. Part of this knowledge is

[63]Overcoming language cultural barrier e-commerce, *available* at: https://www.talk-business.co.uk/2017/01/10/overcoming-language-cultural-barrier-e-commerce-business/ (last visited on April 11,2020)
[64] *Id.* at 60.

acquired by the buyer and the seller through the use of common language and customs. For example, it is more convenient for buyers to do business with sellers they consider reliable. The blend of language and customs is often called culture. Most researches agree that culture varies from state to state and, in many cases, differs amongst regions within nations. For example, the concept of private property is an important cultural tool that appreciates the laws of many European and North American countries. Asian cultures do not evaluate the private property in the same way, the laws and commercial practices of these countries can, therefore, be very different. All companies should be aware of the differences in the languages and customs that make up the culture of a region in which they intend to do business.

Some errors arising from cultural standards have become typical examples that are regularly cited in international business courses and training sessions. For example, the choice of General Motors for the Chevrolet Nova car favored by Latin "it will not go" in Spanish means "Come Alive." In China, Pepsi's "Come Alive" ad campaign was confusing, this message which presented itself as "when Pepsi sent your ancestors out of the grave."[65]

International web designers have to be very careful in selecting icons to represent collective actions. For example, in the United States, a shopping cart is a good symbol to use when creating an e-commerce site. However, many Europeans use shopping baskets when they go to a store and may have never seen a cart. In Australia, people would recognize the image of a cart but the "cart" text would be confusing if used with the image since the Australians call them shopping trolleys. In the US, people often create a hand signal (the index finger touching the thumb to create a circle) saying "OK" or "everything is fine". A web designer may be tempted to use this hand signal as an icon to show that the transaction has been completed or that the credit card has been approved, unaware that in countries like Brazil this hand sign is the obscene

[65] *Available* at: https://books.google.com.au/books?id=Kx9UDt0SMy4C2016 (last visited on May 10,2020)

gesture.[66]

The cultural nuances of simple design decisions can be dramatic. In India, for example, it is not appropriate to use the image of a cow in a cartoon or other comic script. Potential consumers in Muslim countries may be offended by a photo showing bare, arms or legs. The colors or design elements of web pages can also be problematic. For example, white, who denotes purity in Europe and in America, is associated with death and death in China and many other Asian countries. A web page classified into four parts can be offensive to a Japanese visitor because number four is a representation of death in this culture.[67]

2.7.4 Infrastructure Issues

E-commerce continues to face the challenges posed by changes and inadequacies in the support infrastructure of e-commerce. The Internet infrastructure includes computers, networks, and software connected to the Internet and the communication networks through which the message is sent. The industry is government-owned or heavily regulated by the government. In many cases, regulations in these countries have slowed the development of telecommunications or limited the expansion of this infrastructure to a size that cannot reliably support internet traffic.

The issue is telecommunications infrastructure and technology adoption varies greatly around the world. Many developing countries still suffer important infrastructure challenges, including low internet penetration, high access payments and unstable connections. Approximately one-third of online respondents in the study (32%) say their connection is not stable enough to make them comfortable purchasing online. In some developing markets, this figure approaches or exceeds 50%, including in Saudi Arabia (55%), India (36.5%), Nigeria (49%), South Africa (48%), Mexico and the Philippines (47% each). In certain markets, mobile devices have been critical to e-commerce

[66] *Id.* at 37.
[67] *Id.* at 38.

growth, bringing many new and underserved consumers online and their importance will continue to grow.[68]

The availability of internet is root of digital economy and digitalization of economy. For instance, to reduce Indian economy's dependence on cash, it is essential that the internet infrastructure must be better. First, a large part of the population is still outside the banking net and not in a position to reduce its dependence on cash. According to a 2015 report by PricewaterhouseCoopers, India's unbanked population was at 233 million. Even for people with access to banking, the ability to use their debit or credit card is limited because there are only about 1.46 million points of sale which accept payments through cards.

Lack of infrastructure is a serious obstacle to the development and uptake of electronic commerce. The high cost of installing electricity, the cost of computers and the cost of installing fiber optic cables for cheaper and faster internet access, the lack of knowledge of the benefits of using credit and debit cards, the concentration of challenges faced by the ISP in delivering physical goods are the main obstacles that leave most people with the option of using mobile, hence the rise of mobile commerce. M-commerce is facing one of the biggest challenges of the lack of network repeaters, making mobile phones difficult to use in some places.

2.8 Advantages and Disadvantage of E-Commerce

Economic growth and technological development are tied together and represent two sides of the coin. The Digital revolution has sea changes in the current market structure in the world of business. The impact of electronic commerce (e-commerce) on shopping, business collaboration, and customer services as well as on the delivery of various services and goods is so dramatic that almost every organization is affected.[69]

[68] *Available* at*:* The Nielsen Global Connected Commerce Survey, January 2016 (last visited on May 10,2020)

[69] *Available* at https://www.iiste.org/Journals/index.php/JIEA/article/download/39820/40939 (last visited on April 12,2020)

E-commerce is totally eco-friendly as compared to the store and we can say that e-commerce is green commerce in which there is no use of such material that may harm our environment. It is because in traditional commerce we visit a store at a time of shopping, we receive a bill, receipts, coupons etc. These are paper material who harms our environment a lot and that is the reason why e-commerce bought such services which are much eco-friendly, paperless, and effortless to maintain.

E-commerce innovations in human history have brought many benefits to organizations, individuals and society. These benefits are have just begun to materialize, but they will increase significantly as e-commerce expands. The major benefits of e-commerce are discussed below:

2.8.1 Advantages for traders

- In recent times, e-commerce has grown in popularity worldwide as many advanced technologies have been introduced into its ambit. In order to build a market presence or strengthen an existing market position e-commerce companies require to provide cheaper and more efficient distribution chain for their products or services. The innovation of e-commerce has impacted the conservativism underlying traditional markets and economies as a whole, since it has the potential to attract small traders at low cost investments to start or expand a business. We all have seen during the COVID-19 pandemic, many small traders, even in rural, less developed areas have started their business by delivering door to door services through an e-commerce business model. Before COVID -19 small traders had their apprehensions as to how to start online services with meagre resources and lack of infrastructure but the pandemic has helped them realise the possibilities that e-commerce has to offer them. Therefore some of the critical advantages of e-commerce with regards to traders is as follows:

- The low set-up costs attract start-ups to participate in e-commerce. One need not have a physical store to view their products as they can easily view them on their website. In addition, online businesses rely on websites and are highly automated, therefore fewer employees are needed.

- The e-commerce company can immediately take orders 24 hours a day, 7 days a week continuously with minimal costs. This also provides an advantage in the event of expansion in foreign markets when the hourly difference-making more difficult the contacts between the companies. It also improves communication with consumers who don't have to stick to a strict schedule so they can get information and place orders anytime. E-commerce allows consumers to make purchases or other transactions 24 hours a day, all year round, from almost any location.[70]

- The digital or IT network is not limited by borders, does not belong to anyone and the costs of access and publication are extremely low. Communication with a consumer at the opposite pole of the world is as easy as communicating with someone in the next room. Every manufacturer can now sell their products and services in any country through the website and no contact is required with large investments or local companies.

- In e-commerce, international markets are full of services. The global network is not bounded by borders, belongs to no one and the costs of access and publication are extremely low. Each manufacturer can now sell its products in any country through the website and no contact with local companies or large investments is required. Another advantage is the lower operating costs, these costs can be significantly reduced by automating the ordering process. There is also the possibility of total automation through integration with the administration system, thus

[70]Emerging trends in electronic-commerce, *available* at: https://www.toppr.com/guides/business-environment/emerging-trends-in-business/ electronic -commerce/ (last visited on May 10,2020)

leading to an increase in the overall productivity of the company.[71]

- An e-commerce business reduces the labor and other costs in many divisions, including document preparation, conciliation, mail preparation, phone calls, data entry, extraordinary and surveillance expenses. E-commerce can help manage operating costs in many areas, thereby decreasing the cost of individual transactions. The use of e-mail and electronic invoicing represent a significant saving compared to traditional methods.

- Comparing with an individual the computer will not only keep the name and personal data of all consumers as well as their preferences being capable to adopt the offer and product presentation according to each consumer's profile. The study of the consumer on the internet may be achieved using all available data like location, type of browser and operation system, the website where they do come from navigation habits but the consumer will not realize at all that they are subject to such studies. This is why many consider this as a violation of the personal intimacy.[72]

2.9 Disadvantages for traders

While e-commerce may initially seem to solve all your business problems, but moving from a physical location to an online mode has some drawbacks which are the following:

- Certain aspects of electronic commerce do not correspond perfectly to the positive or negative aspects of the subject. Unique problems present an advantage for buyers, adding difficulties for businesses. Consumers can buy, but the business can be affected in another way.

[71] E-commerce advantages and disadvantages, *available* at: https://us.accion.org/resource/e-commerce-advantages-and-disadvantages/ (last visited on May 10,2020)

[72] Advantages and disadvantages of e-commerce, *available* at http://www.esalestrack.com/blog/2008/09/advantages-and-disadvantages-of.html/ (last visited on May 10, 2020)

- Price comparison is a big advantage for online shoppers who can limit businesses. Consumers can compare prices with a single click, rather than crossing the city to visit another store. Many buyers will be looking for the lowest price ever, and if you can't offer it, you'll likely lose the sale.

- Although you can offer lower prices, companies that compete in such price wars will have lower profits. There is nothing intrinsically linked to discounts in e-commerce, the way in which the online market has grown has pushed prices down. Buyers love the lowest prices, but sellers don't.

- Shipping is convenient for consumers but adds burden to the business. Buyers like to have the items delivered directly to their location, but the logistics of delivery add significant pressure to e-commerce business operations. The more you ship, the more the load increases. Logistics and management can become a nightmare, even if the company experiences steady growth in profits and consumer retention.[73]

- As is the case in other activity fields, internet technology has created new fraudulent possibilities. Due to lack of direct interaction with the consumer, the consumer may trade his identity or use false identity to commit frauds. The fraud in e-commerce has created large fraudulent possibilities. In the lack of direct contact, a client may cheat the trader regarding his identity or their real payment possibilities.

- Another significant problem is regarding data security of the company and the individual buyers. A company that has no e-commerce business model need not worry of these reasons as regards the integrity of the administration of informatics systems. The connection to an open network that can be accessed by anyone more or less and access to the confidential data of the local network is raising severe problems. Therefore new risks occurring day by day in digital commerce may cause grave harm to

---

[73] *Available* at: http://www.cch.ca/_resources/pdf/ecommerce_slides_url.pdf/ (last visited on May 10,2020)

traders.[74]

- The launch costs of a digital shop are much cheaper in comparison with those of a brick and mortar store. Though, a company that has yet not implemented an administration informatics system or those where the employees do not have technical skills can confront an unexpected increase in the launch costs due to the necessity of the acquisition of training systems for the workers.[75]

2.10 Benefits for Consumers

Smart tech-savvy consumers are attracted to online shopping by the numerous advantages it offers. Market experts say the overall revenue of online shopping will significantly increase in the coming years. This is because of reduced prices and greater choices. Below are the main advantages of e-commerce that consumers can avail shopping online:

- E-commerce brings great shopping facilities to consumers. It gives the ease to the consumer to make their purchase any time and from any place since online stores are open round the clock. Consumers do not need to carry their goods because goods are delivered directly to their home. They can stay at home shopping comfortably without the need to stand in queues and can download digital products for their instant entertainment. Compared to traditional purchases, consumers don't have to wait for a response from a hotline, but they can easily find answers to their questions on websites. Consumers can save travel time in searching for products from different showrooms.

- E-commerce provides consumers with more choices from which they can select. E-commerce normally provides customers with cheap and good products and services by allowing them to shop in many places and

[74]E commerce disadvantages, *available* at https://www.tutorialspoint.com/e_commerce/e_commerce_disadvantages.htm/ (last visited on May 10,2020)
[75] *Id.* at 72.

conduct quick comparisons. The return of goods is also very easy on online shopping. Consumers do not feel any hesitation in looking at the price of a product or issues in returning the purchased goods. E-commerce companies provide better services to the consumers including several benefits and offers including cash back, replacement of goods or exchange of goods within short time. The digital arena has created global competition among the e-commerce companies and consumers are getting more benefits due to such competitive online markets.[76]

- E-commerce allows consumers to freely interact with other consumers in electronic way of communities and exchange ideas as well as compare experiences. Electronic commerce provides competition, which results in substantial and big discounts for the consumer. It has generally seen that top e-commerce companies like Amazon, Flipkart offer big shopping (Amazon) and big billion day (Flipkart) schemes where massive discounts and offers are extended to consumers creating a big price war between both companies by offering the lowest rate at a comparison to each other.[77]

- The innovation of e-commerce gave a new meaning to the term globalization. For example, in order to buy specific items from Canada it is not necessary to travel to that destination but only to open the websites at the address of a shop that is trading such items. Before purchasing the product the prospective future buyer has cheap and more free access to the offers of the producers or trading companies. Electronic commerce allows some products to be sold at cheap prices, so middle class and less affluent people can buy more and increase their standard of living. The consumer can access to information and products without any restrictions of time, boundaries or weather.

---

[76] Advantages of e-commerce to consumers, *available at* https://accountlearning.com/top-5-advantages-of-e-commerce-to-consumers// (last visited on May 10,2020)

[77] *Ibid*

2.11 Disadvantages for Consumers

Although the benefits of e-commerce are far reaching, the environment of e-commerce is far from perfect. Concerns pertaining to the disadvantages of e-commerce are causing considerable concern for both consumers and businesses. Though cost saving benefits are usually mentioned, however, often there are hidden costs that can quickly convert credit into direct debit. Moreover, technology in itself poses several issues including unreliable network connection. Reasonably the greatest concern in this regard pertains to the security and the loss of privacy, low and remote service levels, and multiple legal issues. The disadvantage of e-commerce for consumers are as follows:

- One of the main roadblocks to the wide acceptance of e-commerce by businesses and consumers alike is the perceived lack of adequate security for online transactions. For example, consumers are providing credit card information for online shopping, however it has been noted that the reports in case of credit card frauds by hackers has increased considerably in the few past years who are penetrating credit card information from the e-commerce databases. The issue is even more worrying since in most cases the information theft takes place much before the seller or the buyer discovers the said problem.

- Ensuring the security of the data is of supreme importance to the credibility of the business and the consumers. These databases usually contain vast information on customer purchasing habits, demographics, credit information, etc.[78] Therefore, it consumers privacy is a matter of large concern not only to the business organisation and consumer but to society at large as well. Even at the simplest level of data, sales information is stored in databases connected to web servers, allowing cyber criminals to disclose information. Since collecting data on the internet is simple, however to track the same can pose itself as an ordeal."

[78] *Available at* http://www.cengage.com/resource_uploads/downloads/061906269X_236713.pdf (last visited on March 3,2017)

- One of the most pertinent advantage of e-commerce that is low engagement of personnel and management through automatic processes also poses the inherent disadvantage of lack of human presence. The physical absence of a seller in the e-commerce business model, creates an issue for the buyer to appeal to another human being in case of doubt and to seek immediate clarification. In this respect some companies have also additionally created programs that are permitting the vocal or visual contact between customers and employees during the customers visit on the web site.[79]
- One of the main disadvantages of an e-commerce portal is that a customer is unable to try and perceive the product for his own satisfaction. Often, the senses are not able to perceive properly what is being offered online without physically verifying the product. This is also because most customers have the habit of only buying in physical stores after trying a product several times and therefore they seem perplexed by the idea of buying something that they have never seen or tried before. When people lack the tangible feeling, the fear that the product does not meet the expected standards. This makes the consumer a little hesitant before making a purchase.
- One of the common drawbacks of e-commerce platforms is late delivery. When ordering a product, the customer is certain that he will get there within a maximum of seven days or within a certain period. In most cases, this does not happen and the customer may have to continue to wait for it. Therefore, customers often face the issue of incorrect timelines. There are also issues with delivery often causing customers to wait for hours for the actually delivery to arrive. Such situations cause undue harassment and hassle the customer who might avoid transaction from the same e-commerce website in future.

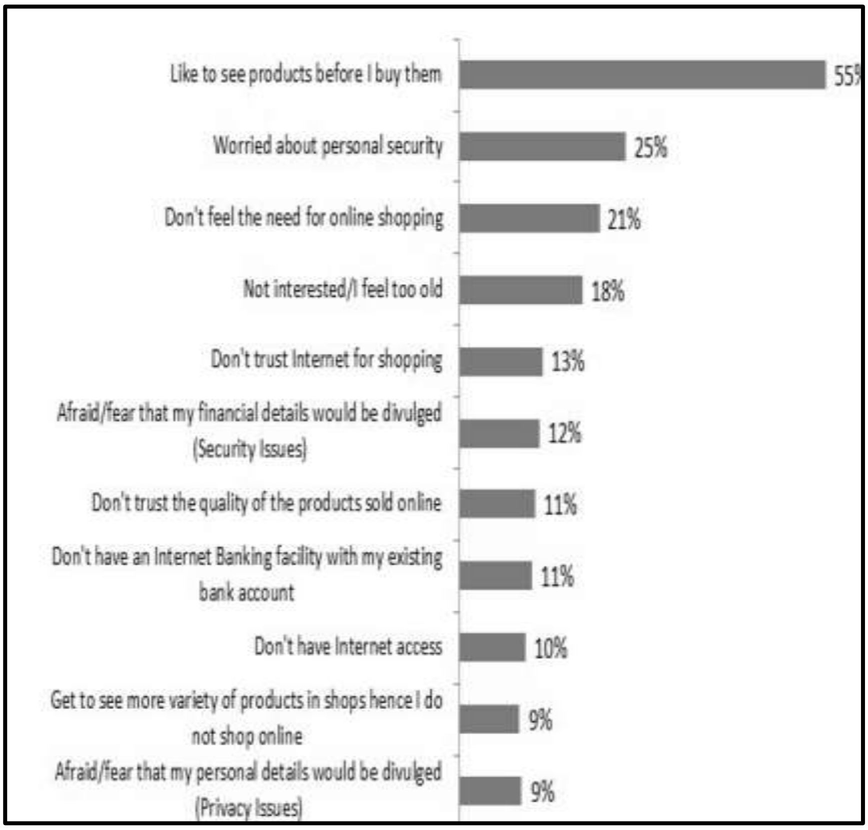
---

[79] E-Commerce advantage, *available* at http://steconomiceuoradea.ro/anale/volume/2006/economie-si-administrarea-afa (last visited on March 3, 2017)

- Extensive information technology regulatory and legal frameworks have been put in place to protect the rights of the seller and the buyer. There are several local laws, cyber laws and legal requirements of which most customers are ignorant and ignore to read. Therefore, they might be affected by the same adversely even without knowing its implications.
- An e-commerce company is heavily dependent on its website for selling products and services. If the website is not properly maintained from time to time or the software is not implemented the consumer might face several difficulties in using the same. An improper e-commerce website can be a soft target for the cybercriminal who keep notice on consumer online transactions which are mostly made by debit card, credit card, and internet banking.

2.12 Reason for not like to buy from E-Commerce websites

As shown in **Figure No. 3,** IAMAI has identified several reasons that are responsible for non-purchase of goods online.



(Source: Report of Online Commerce: March 2017, IAMAI)

There are several reasons that prevent the LFI segment from buying online. Among them, the touch and feel stand out, because approximately 55% of them indicated that they “would see the product before buying it”. Another key reason which is a matter of concern is issues related to personal security. 25% were concerned that online shopping would compromise their personal security.

2.13 Categories of E-Commerce

E-commerce is a new venture for entrepreneurs, sellers and buyers. It is web based venture includes all business activities which are done through digital recourses. At the present time, ‘e’ is gaining momentum..and most of the things, if not everything, is getting digitally enabled. Thus, it becomes very important to clearly sketch the line between different categories of businesses or commerce integrated with the ‘e’ factor. Based on the type of relationship between different sides of commerce, e-commerce can be broken into following major categories:

a) Business to Business (B2B)
b) Business to Consumer (B2C)
c) Consumer to Consumer (C2C)
d) Consumer to Business (C2B)
e) Business to Government (B2G)
f) Government to Business (G2B)
g) Government to Citizen (G2C)
h) Mobile Commerce (m-commerce)

Business to Business (B2B)

Business-to-business electronic commerce facilitates inter-organizational transactions and interaction. This type of electronic commerce requires that two or more commercial entities interact with each other directly or through intermediaries. The intermediary in the B2B e-commerce may be the market makers of and direct service providers, who assist in matching buyers and sellers and striking a deal. The word business-to-business was originally coined to explained the electronic communications between enterprises or businesses in order to distinguish it from the communications between businesses and consumers (B2C). It ultimately came to be used in marketing as well, initially describing only capital industrial or goods marketing.

Today it is widely used to cover almost all services and products used by enterprises. The business application of B2B e-commerce can be utilized to facilitate almost all facets of interaction among organizations, such as purchasing and procurement, supplier management, inventory management, and service and support. It can be a supplier-centric, buyer-centric, or an intermediary centric. Now, it forms a major segment of total e-commerce volume. Value per transaction is high in B2B e-commerce when compared with other models. Today, B2B is the most popular model all over the world. In India, B2B e-commerce is fast flourishing. Some of the most important players in India are Maruti Udyog, Telco, Bajaj Auto, Kinetic, etc. According to ICRA in 'The Indian internet Business Report', the B2B e-commerce turnover represents over 90 percent of the total e-commerce activity in the country.[80]

Business to Consumer (B2C)

In this model, the exchange of products, information or services takes place between business and consumers in a retailing relationship. Some of the first examples of B2C e-commerce were amazon.com and dell.com in the USA, lastminute.com in the UK and flipkart.com, snapdeal.com in India. In this case, the 'C' represents either customer or consumer. B2C e-commerce has enabled not only existing merchants to enhance their potential consumer base, but has also spawned a number of successful business organisation operating only online."

Traditional online B2C commerce, after suffering from the crash of the "dot-com bubble" at the start of the decade, resulted in the survival of a number

[80] *Id.* at 49.

of successful players and B2C e-commerce is now considered a natural and even essential sales channel. Businesses from all operational sectors, from tour to insurance industries, have found that online B2C commerce is an effective and cost-efficient way of doing business. Successful companies conduct online B2C commerce include both brick-and-mortar merchants, like Barnes & Noble, to whom the Internet is just another sales channel complementing the existing channels, as well as a new group of traders, like Amazon, to whom the Internet is the only sales channel.[81]

Consumer to Consumer (C2C)

This model envisages business transactions being carried out between several individual customers who are often consumers. For example, someone who wants to buy used car and someone who wants to sell a used car can meet at C2C web store. This exchange can include third party involvement, as in the case of auction web site OLX. In this category electronic tools and infrastructure are employed to support transactions between individuals. Important differentiation is that no business organization is involved, e.g. automartindia.com focusing on automobile, propertymartindia.com focusing on real estate.[82]

Consumer-to-consumer e-commerce can be explained as individuals doing business in an digital environment, typically utilizing the Internet in one way or another.

Consumer to Business (C2B)

This is the exchange of products, information or services. from individuals to business. A classic example of this would be individuals selling their services to businesses.

---

[81] *Available at* http:// www.groundswell.fi/sim/academic/(sim)%20From%20B2C%20to% 20C2C% (last visited on January 03, 2017)

[82] What is C2C, *available at* https://www.businessnewsdaily.com/5084-what-is-c2c.html (last visited on June19, 2021)

Business to Government (B2G)

This model is a part of e-governance. Under this model, all the information and services are provided by the Government to the business organizations through a huge network of government websites. A commerce organization can get information about business rules, permission, and requirement required for starting a new business, and other specifications. A business organization can also download the different forms and submit it offline or online to the related office.[83]

Government to Business- (G2B)

Here, the exchange of information, services and products takes place between business organizations and government agencies on-line. This may include:

- E-procurement services, in which businesses learn about the purchasing needs of agencies and accordingly provide services.
- A virtual workplace in which a business and a government agency could coordinate the work on a contracted project by collaborating online to coordinate online meetings, review plans and manage progress.
- Rental of online applications and databases designed especially for use by government agencies.

Government-to-Consumer (G2C)

It is also known as e-government. Here, Government websites offer information, forms and facilities to conduct transactions for individuals, including paying bills and submitting official forms online such as tax returns.

Government-to-Government (G2G)

G2G is also a form of e-government. It features, Government-to-government transactions within and between nations, linking local

[83] Online ecommerce tips.blogspot, *available at* http://online-ecommerce-tips.blogspot.in/2010/06/4g2b- government-to-business.html (last visited accessed on March 5, 2017)

governments and also international governments. Here it is necessary to understand e-governance since it is a system to provide transparent and accountable services to citizens through a digital platform.

2.14 E-governance: A government-citizen universe

Electronic governance or e-governance is a system of information and communication technology (ICT) for delivering government utilities services, exchange of information, services communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework.[84].

E-government reduce costs, achieved all companies to interact with the government. Electronic commerce saves time compared to human doing business. No need for driving to government and no waste of time.

2.14.1 Categories of e-commerce at a glance

CATEGORIES	DETAILS	EXAMPLE
B2B	e-commerce model in which all the participants are organizations	Alibaba.com, BtoBOnline.com, IndiaMART.com
B2C	e-commerce model in which businesses sell to individual shoppers	Futurebazaar.com,flipkart.com, Amazon.com sells products to customers through their websites
C2C	e-commerce model in which consumers sell directly to other consumers	Olx.com,Quicker.com in which consumers trade with each other through an online marketplace

[84] E-governance , *available* at https://wiki2.org/en/E-governance (last visited accessed on March 5, 2017)

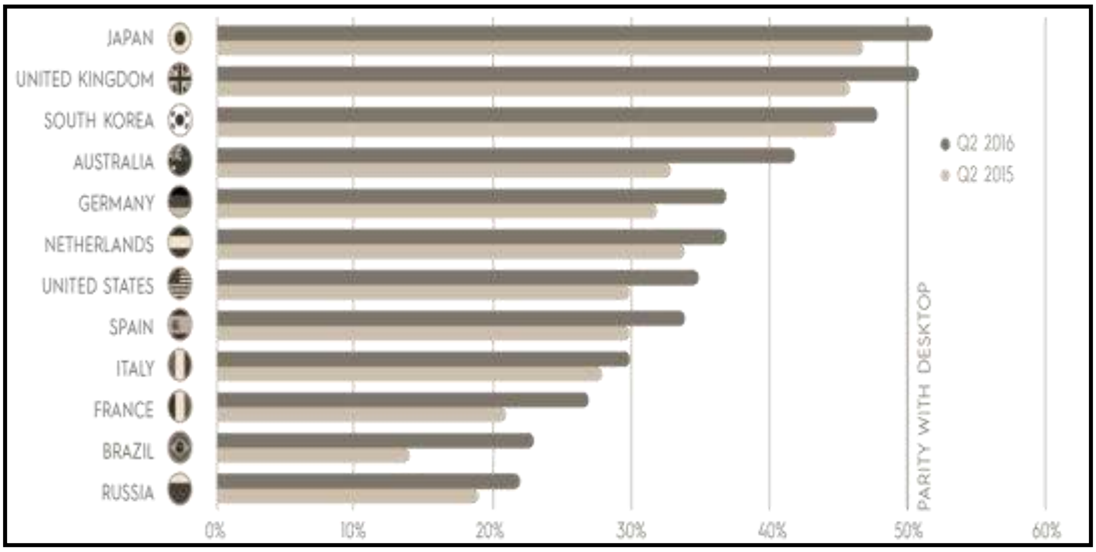
C2B	e-commerce model in which consumers present themselves as a buyer group.	SpeakOut.com IT freelancer who demos and sells his software to a company
B2G	Commerce between companies and the public sector agencies. Websites are accredited by the government and provide a medium to businesses to submit application forms to the government.	Such a business pays taxes, files reports, or sell goods and services to government agencies
G2B	Business model that refers to government providing services or information to business organizations. Government uses B2G model websites to approach such business organization. Such websites support auctions, tenders and application submission functionalities to state a few.	DPIIT G2B Portal is an integrated platform providing access to a number of Government to Business (G2B) services for filing of Industrial Entrepreneurs Memorandum (IEM) and Industrial License (IL) applications Online.
G2C	The way in which citizens can obtain services and purchase products from the government through electronic media	Applying for certificates, licenses, permits, marriage registration, for submitting information are a few examples
G2G	Government-to-Government transactions within and between nations, linking local governments and also international governments	Support e-government initiatives by improving communication, data access and data sharing between countries and local government.

2.15 Mobile Commerce (M-Commerce)

M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs). Known as next-generation e-commerce, m-commerce enables users to access the internet without needing to find a place to plug in.

M-commerce transactions continue to grow and the term includes the purchase and sale of a wide range of products and services, such as online banking, payment of bills and delivery of information. Consumers typically use Google, emails, and/or social media promotions to initiate their online shopping searches, leading them to mobile browsers. As a result, traffic and purchase conversions through browsers outperform those through mobile applications. However, it is important that mobile applications are used in conjunction with mobile websites to enhance consumers' overall shopping experience. For example, mobile applications can be used to facilitate customer engagement that may lead to repeat buyers.[85]

The Figure 5 shows the Mobile data regarding E-commerce in different developed countries.



source:https://jmango360.com/must-know-mobile-commerce-trends-2017/

[85] *Available* at https://issuu.com/ninojosephmihilli/docs/about_mobile_commerce_by_nino_josep (last visited on November18, 2016)

In India, mobile commerce is undergoing an exciting transition. The country has seen an impressive increase in daily trade via mobile devices. A market report released in 2019 by consulting firm statista estimated that the m-commerce market worth $ 2.9 trillion in 2020 and has reached approximately $ 3.56 trillion by 2021. India is now one of the top five regions for the Google Play store, as more than 1.2+ billion people look to search, interact, and shop on the go via their smartphones and other devices.[86] Indian m-commerce consumers share almost 51 percent of digital commerce via smartphones compared to 39 percent in the world.[87]

2.16 How Electronic Commerce is making a difference

E-commerce has been making huge gains and has infiltrated for all intents and purposes, each circle in Indian market. With the guarantees of straight forwardness and accommodation, it has given both the occupants and foundation something to be amped up for. Indian government is additionally dedicated to support the digital transactions and try to make 100% digital literacy in the nation**.**

Demonetization prompted a higher reception of UPI and wallet-based instalment benefits have played a catalyst role to the cashless exchange medium. While customers from metros might be ahead as far as utilization of computerized wallets, this pattern has picked up with customers across urban India. While the underlying effect of demonetization may have given the push the online instalment administrations required, when the impacts of money crunch were gone and the circumstances balanced out, a sizeable segment of the populace returned to utilizing money again as the favored method of exchange.

[86]Indias m-commerce landscape in 2016, *available* at https://venturebeat.com/2016/01/16/indias-m-commerce-landscape-in-2016-hyperlocal-and-growing-fast/ (last visited on May 10,2020)
[87] How M-commerce Is Changing the Landscape of E-commerce in India, *available* at https://www.entrepreneur.com/article/346340 (last visited on June 19, 2021)

So as to take greater steps towards turning into a computerized economy, there is a need to boost the organizations and shippers to make advanced instalments as the favored method of exchange. Another significant aspect that should be remembered is the security of exchange as there is still a ton that should be done to guarantee that the exchanges are ensured and secured with administrative structures that can guarantee the Indian purchaser that his exchanges won't be undermined. The job of online security has gotten progressively critical as of late as cell phones have risen as the key gadget for online exercises and online exchanges.

2.17 Conclusion

E-commerce is a emerging trend in modern business system. No doubt e-commerce has changed the business phenomena in the world; it is a revolution for change the concept of pigeon hole theory of business and breaks the traditional system of consumerism. The arena of e-commerce are appearing in all form of business, from customer service to new product design. It empowers new aspects of information based business processes for reaching and interacting with customers online through advertising and marketing, online, order taking and online customer service etc. It can also decrease cost in managing orders and interacting with a wide range of suppliers and trading partners, areas that typically add important overheads to the cost of services and products.

As we know that every coin has two facets, similar is the case with e-commerce. The plethora of advantages that it has to offer, it also has its own serious issues.

In the upcoming chapter, the researcher explores the issues faced by the consumer in e-commerce particularly with regards to data privacy. The researcher will take an analyses of the existing aspects of consumer protection, its issues and problems which adversely affects the potential growth of e-commerce in the present day and age.

CHAPTER-3

CONSUMER RISK: AN ISSUE IN E-COMMERCE

CHAPTER-3

CONSUMER RISK: AN ISSUE IN E-COMMERCE

Technology: The knack of so arranging the world that we need not experience it.

—Max Frisch, Homo Faber

3. Introduction

This chapter presents the different kinds and forms of risks faced by parties engaging in electronic business transactions. Furthermore, the researcher aims to explore why e-commerce businesses facing rapid growth or changes in their corporate information systems may face an increased risk of insecure systems. Thus, the focus of this chapter is on risk identification of online transaction and consumer issues[1] to a wide range of users from various internet sources and the associated legal gamut in that regard.

Good consumer service is synonymous with good customer loyalty and good word of mouth. The explosion of e-commerce transactions offers great opportunities for all types of businesses. The internet has attracted both entrepreneurs and companies who are looking for a new business model and consumers who are looking for a non-stop facility of shopping. E-commerce has established a new and attractive relationship without the need of a brick and cement structure to interact within. Thus, e-commerce has come forth as an exceptional opportunity for all those seeking to grow their revenues and to expand their customer base.[2]

It is not limited by factors such as occasion, time, distance and thus it allows a business to enter and grow in any new customer circle. Such a business model is no longer restricted to a physical market and rather enters

[1] Marilyn Greenstein and Todd M Feinmam *Electronic Commerce Security, Risk Management and Control* 131 (Tata Mcgraw-Hill Copmany Limited, New Delhi 2000)

[2] Janice Reynolds, *The Complete E-Commerce Book: Design, Build, & Maintain a Successful Web-based Business*,233 (CMP Books, 2nd edn., 2004)

into the realm of portable trade which is easily accessible and available from any place and at any point of time. Moreover, the digital market offers a simple and transparent mechanism for money transactions with the ease of digital payments and convenient exchange and refund policies. All Banks have put in place work areas and portable organizations to facilitate such online transactions and exchanges. Worldwide e-shopping mammoths Amazon, e-bay, Alibaba and domestic e-shopping platforms such as Flipkart, Snapdeal, Nykaa, Myntra, etc., have built up an entire range of options and opportunities. It has transformed the way the country indulges in shopping, especially in urban and semi-urban areas. The RBI has permitted several banks and portable wallets for money to undertake money related exchanges such as ICICI pockets, SBI Yono, Paytm, MobiKwik, Vodafone M-paisa, Phonepe to name a few. With regards to instant messaging, WhatsApp has come forth as the most popular mobile messenger app worldwide. Recently WhatsApp has introduced the facility of instant money transfer as well which is increasingly gaining popularity. In today's time, the consumer no longer needs to allot time for undertaking e-shopping. At any waking hour of the day or at any hour late in the night, the customer can experience the digital work by just a click. The consumer is flooded with constant offers and sales, enticing him to come back and purchase time and again.

Constantly, with such high volume of personal financial data being circulated it has exposed millions of customers to the possibility of digital crimes. With data being constantly shared and circulated and e-cash moving in and out of accounts, they become high susceptible to be tapped into by cybercriminals. Therefore, to meet such persisting threats, all e-commerce websites are expanding their technical base and data security facility in order to secure such digital transactions and protect customers. From selling contraband substances, to providing lawful and unlawful services, to matrimonial websites and e-shopping, almost everything and anything under the sky is available online. However, this also means that with the increase in such transactions the susceptibility of misuse of the same may become even more possible. Hacking e-mails, bank accounts, personal data, debit and credit card are some of the most common cybercrimes in e-commerce.

Though risk in this regard exists in each and every format however its probability and scope differs depending also on the nature of the networking technology. In case of intranet, the network is private and is insulated from global internet. It is usually utilised by large enterprises and organisations as private networking technology for intracompany telecommunications. In such case, the risk is limited solely at the enterprise level. However when both intranet and the internet or extranet are linked, the risk may extend since it will be exposed to external perpetrators as well.

Unfortunately, legitimate selling agents and legitimate customers are not the only parties connected to the internet. Other parties lurking on the internet include various perpetrators, both internal to legitimate buying and selling agencies and external independent ones, with a number of techniques and motives for engaging in fraudulent, harmful acts on the internet which affect both selling agents and their customers.

3.1. Who is a Consumer?

The term “consumer” is defined as “a person who buys, has the ability to buy, products and ventures.” A consumer is a person who purchases goods or services for personal use and not for production or resale. A consumer is someone who decides to purchase an item from the store or not or someone who is influenced by advertising and marketing to buy anything. Every time someone goes to a store and buys a shirt, toy, drink, or anything, they decide to buy as a consumer. Consumer refers to anyone who buys certain goods for payment, to whom it has been paid or promised to pay or partially paid and partially promised to pay or found in a deferred payment system. It involves a beneficiary of this type of property other than the person who buys such goods for payment or promised or partially paid or partially promised or somehow deferred payment when this type of use is made with the consent of that person but does not include a person who uses such services for commercial purposes, resale or hire or use certain services for consideration.[3]

The law mainly uses consumer as a concept in relation to consumer protection laws and the definition of consumer is often limited to living persons (i.e. not to companies or businesses) and excludes commercial users. A typical legal justification for consumer protection is based on the concept of repression of market failures and inefficiencies, as an unequal bargaining power between a consumer and a company. Concern for consumer interests generated consumer activism, in which organized activists carry out research, education and defence activities to improve the offer of products and services.[4]

As per the new Consumer Protection Act, 2019, a person is called a consumer who avails the services and buys any good for self-use. Deserving to mention that if a person buys any service and goods for resale or commercial purpose, he is not deemed to be a consumer. The new act deals with all types of transactions i.e. offline and online through electronic means, teleshopping, multi-level marketing or direct selling. However, the Act does not cover a person who obtains a good for resale or a good or service for commercial purposes.

Section 2(9) Consumer Protection Act, 2019 provides for six rights to the consumer:

(i) Be protected against the marketing of goods and services which are dangerous to life and property;
(ii) Be informed of the quality, quantity, potency, purity, standard and price of services or goods
(iii) Be assured of access to a variety of goods or services at competitive prices;
(iv) Seek redressal against unfair or restrictive trade practices and services.
(v) Consumer awareness

[3] Who is a consumer, *available at* www.consumerrights.org. (last visited on May 2 , 2020)
[4] *Ibid*

(vi) Right to be heard and to be guaranteed that consumer needs will get due thought at an appropriate forum.

3.1.1 Types of Consumer

According to the nature of consumption, consumers are of following types:

a) Direct Consumers

The initial phases of civilisation were marked with producers producing all the basic necessities for themselves and their families only. All the essential needs such as food, clothing and shelter that they themselves produced was for their own consumption and that of their families. Therefore, producers solely produced goods for their own consumption only and thus were called direct consumers or even direct producers.[5]

b) Consumers by Exchanging Products and Service

Over time and civilization, people understood the importance of trade. Hence, they tried to specialize in a certain product or on some products, then tried to trade the product by exchanging it with other products. This system of exchange of products came to form the barter system. This created the notion of a negotiable surplus, which means that producers not only produce goods for their own consumption but also certain surpluses which they trade to obtain other products in return. For instance, a farmer who produces pulses did so not only for self-consumption but also to use the additional or excessive produce in order to exchange it with producers of another product.[6]

c) Modern Consumer and E-consumer

Modern consumers only go to the market to buy goods and services that are available in the market in exchange for money. Here manufacturers also produce goods or services that are shipped directly to the market for

[5]Types and importance-of-consumers, *available at* www.economicsdiscussion.net (last visited on May 2, 2020)
6 *Ibid*

consumers. Modern consumers are the outcome of the monetary system.

With the development of marketing technology, the modern consumer becomes an e-consumer. An e-consumer uses digital mediums like a mobile, computer, or other digital devices, to buy services and goods and this is not limited to this but also incorporates the ease of using digital payment systems such as e-wallet, card payment, UPI payment, etc. Today, e-consumer is a paperless consumer who keeps all data in his digital device. This consumer has highlighted the value of this new concept of payment system during the COVID-19 pandemic and the national lockdown. On account of the pandemic, the relevance of such e-commerce has been felt across the nation, including small rural areas. As a result of the lockdown, housebound consumers across the globe turned to e-commerce platforms for all of their essential requirements including groceries, medicines, bill payment, education, etc.

d) Second Hand C2B Consumer

Second-hand Consumer to Business (C2B) is a relatively new trend in the business model of e-commerce, in which consumers sell their used product and e-commerce companies buy that product usually in an online environment. This is a marketplace model to buy and sell used or second-hand products. Second hand C2B marketing has become popular with the advent of the internet and companies like eBay, Etsy, Cashify, OLX, and Quikr.

In e-commerce, the second-hand C2B business model is not the most reliable place. This is usually susceptible to fraud and deception and often buyers and sellers do not trust each other. Moreover, scammers can trick consumers on their websites by using false branding and misleading photographs.

The main problem in buying and selling second-hand C2B in e-commerce is the lack of quality control. No one can guarantee your product value and the protection of money. Furthermore, the lack of refund policy is not clear or transparent. So if something goes wrong, there is no way one can take action against a dishonest purchaser. Under the new Consumer Protection

Act, 2019 second-hand C2B consumer is not considered as a consumer, thus, the act does not protect a consumer who bought or sold the used product. In India, this model is fast growing and e-commerce is a million rupees business every year. Furthermore, there is no protection for such consumers if an e-commerce company cheats the consumer or subsequently reduces the price of the goods on unscrupulous basis and sets out unfair terms and conditions. Consumers also suffer on account of practical issues such as long delays in pick-up or delivery, mishandling, etc. or reduces or increases the price unreasonably or adds additional hidden costs, in such cases the consumer has no recourse for grievance redressal.

3.1.2 The Issue of Rights Concerning E-consumers

The rapid development in e-commerce business has significantly caused a noted rise across the globe in the e-consumer category. In case of an act of selling and buying of products or services on the virtual electronic world the buyer is known as an e-buyer, a seller is known as an e-seller, the retailer is known as an e-retailer, a consumer is known as an e-consumer and the transaction is known as an e-transaction.

Due to the lack of physical interaction and the complex nature of web-based shopping, e-consumers require at any rate a similar degree of insurance as given under law and practice to the customary method of business. Holding the attributes of the conventional client, the e-customer expressly utilizes the internet and a totally different arrangement of novel capacities centered towards web-based shopping of items and administrations. This wonder depends on the presence of two fundamental premises:[7]

- Web-based services, including e-commerce, that relies on complex, large scale systems consisting of thousands of computers, heterogeneous networks, and software components;

[7] Econsumer.gov: e-consumer - Report international scams online!, *available at* /www.econsumer.gov/ (last visited March 2,.2020)

- Users, i.e. electronic consumers or e-customers, who communicate with the previously mentioned digital services unpredictably and stochastically.

On account of the uniqueness of e-commerce in terms of place and nature of business or medium of business, specific practical difficulties like place of business, jurisdictional issues, non-availability of common dispute resolution system persist. Furthermore, on account of the boom in international transactions through the electronic system (e-shopping), i.e. the buyer of one nation purchase from seller of another nation or vice-versa, etc. Electronic transactions or e-commerce has become indispensable and certainly requires special measures that are not provided in the existing consumer legislation.

The right of consumers and e-consumers though appear similar in theory but are uniquely different in operation and enjoyment. Due to the associated ease in e-commerce and e-transactions, the number of e-consumer are also growing at a high rate and within a very short period it may defeat the physical consumer base. Considering these aspects strong protective mechanisms are required to be set up and stringent measures in the form of laws need to be framed otherwise it will not only affect the e-consumers but also affect the business infrastructure and the economy of the country in the long run.

3.1.3. The need for protection of rights of E-Consumer

The number of e-consumer are growing at an exponential rate in the present times and due to its user-friendly nature but at the same time, the associated risk and incidents of cybercrimes are also increasing. These risks have taken up various forms and therefore a wide range of protective laws and measures need to be put in place against the manifestations of programmers, duplicate social media account, stolen of private information without consent, masking, caching, cloning of debit and credit card, virus threats, etc. However, some problems make the protective measure indispensable in this respect and require immediate and effective protection mechanism. It ranges from rules for opening bank accounts to standards for the manufacturers, safety norms for goods and services, etc. The government needs to actively regulate, frame laws, provide for their proper enforcement and grievance redressal in case of e-commerce related organisations as well such as the stock market, banking sector, internet service providers and data companies ensure e-consumer protection and data privacy.

3.2. Issues and Challenges to Laws in New Technology

The biggest challenge before the law is to maintain pace with technology. While talking about crimes relating to the internet, crimes like fraud, defamation, data-stealing would nevertheless be governed by the existing technology-neutral criminal laws and regulation. These are crimes with all the elements of an offline offence with the difference that the internet is used as the facilitator for such a crime.

The second kind of crime is the one directed at computer networks and data. These are the crimes that need to be newly defined and prohibited for the purpose of maintenance of order. They include unauthorized disruption of computers and networks, the heart of what most people consider cybercrime. It occurs when an entity, without permission, interferes with the functionality of computer software or hardware. They include viruses, worms, logic bombs, Trojan horses and denial-of-service attacks.[8] Unauthorized access to computer programs and files are the other categories of offences directed at computers.[9]

For example on April 7, 1999, visitors to an online financial news message board operated by Yahoo!, Inc. got a scoop on PairGain, a telecommunications company based in Tustin, California. A post under the subject line "Buyout News" said that PairGain was being taken over by an Israeli company was posted. It provided a link to what appeared to be a website of Bloomberg News Service, containing a detailed story on the takeover. As news of the takeover spread, the company's publicly traded stock shot up more

[8] S.k. verma and Raman Mittal (eds.) *legal dimention of cyberspace* 231 (Indian Law Institute 2004)
[9] Neal Kumar Katiyal (eds.) *Criminal Law in Cyberspace*, 1021-1031 (*Univ Penn L Rev* 1003)

than 30 percent, and the trading volume grew to nearly seven times its usual. There was only one problem: the story was false, and the website on which it appeared was not Bloomberg's site, but a counterfeit site. When news of the hoax spread, the price of the stock dropped sharply, causing significant financial loss to many of the investors who had purchased the stock at artificially inflated prices.[10]

Many challenges of making laws related to technology-based issues is that they tend to get outdated very soon. Therefore, it is desirable that laws, as far as possible, must be drafted in a technology-neutral way. Again it is against equity and fairness if offline conduct is governed differently from online conduct. This gives rise to the possibility of crime shifting from one place to the other if there is an inconsistency in laws. Consistency between the two laws is, therefore, desirable. Laws must also cater to the need of prevention and investigation of crimes. For instance, with the advent of telephones, wire-tapping laws were introduced; similar laws to deal with unlawful conduct on the internet would become necessary.

Similar is the case with the use of technology like encryption. Modern encryption would make encrypted documents almost impossible to read, thus making it a safe means of communication for criminals. In the interest of law enforcement, some kind of regulation on this would be desirable. Something like an order to manufacturers to combine encryption with a key recoverable feature, which allows lawful and immediate access to plaintext of encrypted communications and electronically stored data, say made available on a court order.[11]

Case: A major corporate research laboratory used the internet to search for information on new product plans. In a test of the system, a security specialist illegally accessed the internet communications of two researchers and

---

[10] A Report of the President's Group on Unlawful Conduct on the Internet, *available* at www.usdoj.gov/criminal/ cybercrime/ (last visited on May 15, 2020)

[11] Law & Technology: Risks and Opportunities from the Tectonic, *available* at: www.whitecase. com (last visited on May 15,2020)

recorded their search inquiries and the internet Uniform Resource Locator (URL) addresses they visited. The specialist then gave the key word search inquiries and URL's to an independent researcher in the same field, who immediately hypothesized the type of product the company was working on and the new dimension of the product under development. When informed of the results, the laboratory researchers confirmed the hypothesis.[12] This is just one example of an incident where the internet can be used to access information and commit a cybercrime, even without the person knowing of it.

The issue, challenges of e-consumer can be discuss in two parts for its better understanding:

- Cyber tort
- Cybercrime

3.2.1. Cyber Tort

Tort more less mean wrong …one of my friends said that torts are the course which proves that your mother was right.

As Scott Turow, American lawyer and author, states that torts are wrongful actions through which society compensates those who have suffered injuries as a result of the wrongful conduct of others. The basic aim of tort law is to provide remedies for the invasion of several protected interests. Society recognizes an interest in personal safety, and tort law provides remedies for acts that cause physical injury or that interfere with physical security and freedom of movement. Society recognized an interest in protecting property, and tort law provide remedies for acts that cause destruction or damage to property. The society also recognizes an interest in protecting certain intangible

[12] David L, and Andra , *et*.al., Computer *Crime: An Emerging Challenge: An Emerging Challenge for Law Enforcement, Cybercrime and Security*, 1.5-3 to 1.5-4 (1998), cited by S.k. Verma and Raman Mittal(eds.) *legal dimention of cyberspace* 232 (Indian Law Institute 2004)

interests, such as personal privacy, family relation, reputation, and dignity and tort law provides remedies for invasion of this interest. [13]

In a famous legal treatise on torts, Prosser and Keeton wrote, "broadly speaking, a tort is a civil wrong, other than a breach of contract, for which the court will provide a remedy in the form of an action for damages." To keep in mind this that torts are civil wrongs, as opposed to criminal wrongs. No one goes to jail for committing a tort, although the same behavior that resulted in a civil tort still may separately also form the basis for unlawful action. i.e., if person X stabs and kills person Y, person X may be convicted of the crime of murder and be punished accordingly, however, person X may separately be found liable to the estate of person Y in a civil suit for the tort of wrongful death, and have to pay damages to the estate.[14]

On the other hand, tort suits differ from contract suits since in the latter it generally involves documentation as evidence whereas in case of tort suits most often it does not. A suit based on a personal injury suffered in an accident, for example, generally arises from something that happened suddenly and without warning. The parties typically do not know each other before the accident occurs. They have no reason to have documented their relationship in any way. This also explains why tortious disputes are more likely to go to trial than contract suits. Parties to tort suits have no existing relationship to preserve. On the other hand, the parties to a contract generally expect to see each other again after the dispute has been resolved. Instead of engaging in costly and bitter legal battles, they may enter into a settlement because it provides foreseeable benefits. If they are commercial trading partners, they have strong incentives to reach a settlement of a dispute that preserves the mutually advantageous relationship.[15]

[13] Roger LeRoy Mille, *law for e commerce* 75 (,west Thomson learning,page, 2002)
14 E-commerce Disadvantages, available http://www.cengage.com/resource_uploads/downloads /061906269X_236713.pdf (last visited on March 3, 2017)
[15] `India: The Rise of E-Commerce And Intermediary Liability, *available* at: www.mondaq.com (last visited on June 7, 2021)

In the area of torts, as in other areas of law affected by new technology, there are more questions than answers. One of the foremost issues is the question of who should be held liable for a cyber tort i.e. a tort committed in cyber space. For example, who should be held liable when someone in a newsgroup posts a defamatory statement (an online message in which one party attacks another in harsh, often personal, terms)? Should an Internet Service Provider (hereinafter to be referred as ISP) be liable for the remark if the ISP was unaware that it was being made?[16]

Other questions involve issues of proof. How, for example, can it be proved that an online defamatory remark was published since defamation requires a third party to see or hear it. How can the identity of the person who made the remark be discovered? Can ISP be forced to reveal the source of an anonymous comment?

Access to digital mobile networks have become available and affordable for the public at large. Certain digital networks have large capacities and possibilities for processing individual data. The successful international development of these services is partly dependent on the confidence of the consumer that their privacy will not be at risk. The following torts are countable in cyber tort and need to be discuss:

- Defamation
- Negligence
- Breach of Privacy

3.2.2 Defamation

Defamation is important to discuss since it is one of the most commonly committed cyber tort. Defamation is the intentional infringement of another person's right to his good name.

[16] Roger Leroy Miller and Gaylord *Law for E-Commerce* 75 (West Thomson Learning,USA 2002)

It is the wrongful, intentional publication of words or behavior concerning another person, which has the effect of injuring that person's status or good name or reputation in society. A person's good name, status or reputation in society is essentially the general public's opinion of that person. Consequently, his good name can only be damaged if maligning statements are made to someone other than that person: the defamatory statement must be disclosed to a third person.

In general, the requirement of publication is satisfied if the defamatory allegations are made to only one person other than the person whose reputation is being impaired. It is not necessary for the statement to be published in the press or made known to several people: disclosure to one person only is sufficient. Not many people are aware of how easily a defamation action can therefore arise and it is this ignorance or lack of awareness, which increases the risk of defamation over the internet.

Thus, the law assumes that an individual intends normal facts about others. Breaching of this duty in writing of permanent form like digital recording, emails involves the tort of liable and if breaching of duty in oral form is slander. In India, there is only one form of defamation that is punishable under the Indian penal code. As per the section 499 Indian Penal Code Defamation as below:

Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.

When any defamatory statement made by the internet or any other digital medium, it is a kind of cyber defamation, punishable under section 499 Indian Penal Code, 1860. However, the courts have held that there will be no 'publication' unless the third person to whom the defamatory statements were made actually understood their meaning?[17]

Online forums allow anyone under the sun to approach and complain about a business firm. A comment left online could concern the firm's personnel, policies, practices, or products, and it might have an impact on the business of the firm. This is possible regardless of whether the complaint is justified and whether it is true.

If a statement is not true, it may constitute defamation. Defamation is any published or publicly spoken false statement that causes injury to another's good name, reputation, or character. Like other torts, defamation is governed by state law, and the elements of the tort can vary from state to state. As discussed earlier in this chapter, generally, a plaintiff must show that a statement was false, was not subject to a privilege, was communicated to a third person, and resulted in damage to the plaintiff. A public figure must also show that the statement was made with actual malice.[18]

The following are among the areas of risk of exposure to defamation:

a) World Wide Web:

The World Wide Web can now be accessed in most jurisdictions throughout the world. The web results in an instant global publication of information at a very low cost. The information which would not normally have been revealed prior to the dawning of the internet can now be unearthed by practically anyone.

b) Intranets:

Intranets are intended to be used internally by an organisation only and access by outsiders is usually denied. However, organisations forget how easily information from the Intranet can be downloaded and forwarded by e-mail or

[17] Cyber-defamation, *available* at https://www.slideshare.net/TuhinBatra/cyber-defamation, (last visited on March 2,2020)
[18] *Ibid*

otherwise to third parties. The Intranet, therefore, creates a false sense of security.

c) Mailing lists and bulletin boards:

The information posted to a bulletin board can be accessed by anyone. This means that anyone can place defamatory allegations on the bulletin board and that the world at large can read the defamatory allegation.

d) E-mail:

E-mail users generally tend to treat e-mail correspondence as a kind of conversation rather than a written interaction. Caution is often thrown to the wind. Users forget that e-mails are stored and can be retrieved as hard copies and that their contents then cannot be disputed. They forget to the ease and speed with which one message can be circulated to literally hundreds of people and as far as it goes, a defamatory allegation need only be disclosed to one person to become a tort of defamation.

It is possible that a person could e-mail a defamatory remark to the person about whom the allegation is made. The sender may well intend that person to be the sole recipient of the message. The e-mail could, however, accidentally and very easily be sent to hundreds of other people. If the sender could reasonably have been expected to know that the defamatory allegations could be disclosed to other persons then he will still be held liable for defamation even if he didn’t intend to disclose the message to others. This issue has arisen previously in relation to the sending of letters and postcards. The courts have, for instance, held that in the case of a sealed letter which is specifically addressed to one person, the sender would not expect others to open the envelope and read the letter. The sender would therefore not be held responsible for publication. If, on the other hand, the sender sends a postcard and it is read by others, it is self-evident that a postcard is likely to be read by others. Thus, a sender would be aware of the likelihood of an e-mail being seen by many persons and that the sender of defamatory e-mail in this instance would be held responsible for publication.[19]

When determining whether or not defamation has taken place, the only issue to consider is whether the average person of ordinary intelligence in society would believe that the words would injure the person's reputation. The factual situation is not relevant. Consequently, even if there is no damage to the person's reputation in fact, the person who made the allegations can still be liable for defamation. It is, of course, difficult to determine who "the average person" is in a society such as India which is a complex mix of different cultures, attitudes and beliefs. Examples of defamatory allegations include allegations that the plaintiff has committed a crime, is guilty of cowardice, dishonesty, immortality or racism. Any statement which would arouse hatred or contempt in the general public or which could result in ridicule could be classified as defamatory. Once it has been proved that defamatory matter about a certain individual has been published, it is presumed that such publication was unlawful and intentional and that it has damaged that person's reputation. Herein lies the fact that all a plaintiff has to prove in a defamation action is a publication of defamatory matter and the onus is then on the defendant to show that such publication was, in fact, lawful and/or unintentional. The law of defamation, therefore, places a heavy burden on the defendant. Once again, most people are unaware of this burden and this too illustrates the latent dangers which are attached to the internet and e-mail usage.[20]

In essence, the law of defamation attempts to create a workable balance between two equally important human rights: the right to an unimpaired reputation and the right to freedom of expression. The courts have questioned whether the law of defamation as it presently stands can be considered Constitutional, in that a greater value is attached to one's right to reputation than to one's right to freedom of expression. Certain courts have held that the plaintiff should also have to show that the defamatory statements were

---

[19] Rodney D Ryder, *Introduction to Internet Law and Policy*,229 (Wadhwa and Company, New Delhi 1st edn.2007)

[20] Defamation laws and judicial intervention, *available* at: http://ili.ac.in/pdf/paper10.pdf (last visited on May 15,2020)

unlawful and that it should not be for the defendant to justify his conduct by showing that the statements were, in fact, lawful. However, there have been several conflicting decisions on this point and there is accordingly no certainty at this stage.

The most common way in which a defendant can show that his conduct was lawful is for him to show that his statements were true and that the disclosure thereof was in the public interest. These are the most common defences used in a defamation action. If a defendant proves that his statements were true and in the public interest, then his conduct is regarded as lawful and he will not be held liable for defamation.

3.2.3. Defamation and the Media

The liability of the press, or distributors of published information, however, is not so easily shaken. The mass media have always been held liable for defamation even if they are not at fault. If an article is published in a newspaper with the honest, reasonable belief that it is true and it later turns out that it was false and defamatory, the newspaper could still be held liable.[21]

Moreover, social media has become an unrestrained facilitator for circulating fake and defamatory messages. According to a survey, 89% messages and videos are fake and maximum people like to watch and share such videos and messages. It can easily be seen on social media platforms that every minute a fake message against celebrities, top personalities is being circulated all around the world. Recently in the Delhi riots, on account of fake videos and news which was circulated, people acted out and reacted on account of such fake news.

Applying the ordinary principles of defamation to the internet, it is evident that there are several areas where there is a very real risk of liability for defamation. The nature of the e-mail and the use of the internet is such that users are lulled into a sense of intimacy and security and forget the usual

[21]Defamation: Digital media project, *available* at: www.dmlp.org (last visited on May 15,2020)

concerns about openly maligning or insulting remarks about another person. The fact that the user is "alone" with his computer and distanced from other users creates this sense of intimacy and confidence.[22] There is no spoken telephone conversation or dictated correspondence which would normally instill some caution. In addition, the idea that the internet is a free for all cyberspace where there are no limits or boundaries results in the user's sense of social norms and of what is acceptable to society generally being dulled.[23]

3.2.4. Negligence

Several tort suits are based upon an allegation that the injury the plaintiff suffered was a result of negligence by the defendant. The general standard of care used in deciding whether or not a defendant was negligent is that of the 'reasonable person'.

Who is a reasonable person? He or she is a creation of the law. The reasonable person is not perfect or infallible, but rather represents a standard reflecting the virtuous judgment of the community; what the community feels ought ordinarily to be done, as opposed to what ordinarily is done. This strategy to determine the liability of the defendant implies that conduct is the deciding factor and that conduct is to be measured upon visible "norms".[24]

Justice Holmes, in The Common Law, observed that

"*The law considers what would be blameworthy in the average man, the man of ordinary intelligence and prudence, and determines liability by that." However, he added, "There are exceptions... which illustrate the rule"* citing as examples a blind man or a child, who are judged by a standard other than the general reasonable person rule.

Prosser and Keeton[25] wrote that

"*As to his physical characteristics, the reasonable person may be said to*

[22] Defamation social media, *available* at http://mccagueborlack.com (last visited on May 15,2020)

[23] Rodney D.Rayder *Introduction to Internet Law and Policy* 230 (Wadhwa and Company 2007)

[24] Rger Leroy Miller and Gaylord A. Jenta, *Law for E-Commerce* 86 (West Thomson Learning, USA 2000)

[25] Robert Dunne *Computers and the Law: An Introduction to Basic Legal Principles and Their Application in Cyberspace 60* (Cambridge University Press, 2009)

be identical with the actor," and that "conduct of the handicapped individual must be reasonable in the light of the person's knowledge of his infirmity"

So, the defendant's behavior is judged by what it is reasonable to expect that a particular defendant to have done in the given situations. Professionals employed in performing their professional tasks are, of course, held to a higher standard of care than an ordinary person would be if required by circumstance to perform the same tasks. i.e., a physician who happens to come upon a car wreck and administers aid to the sufferers will be expected to do so more expertly than, say, a computer programmer who happens upon a wreck and tries to help.

Children have traditionally been held to standards of care appropriate for their tender age, although several courts have modified this to allow for adult standards of care to be applied to children performing "adult" actions, such as driving motorboats, cars, etc.

Customs may play a role in determining the standard of care to be applied. Proof of a common practice helps in formulating the imprecise expectation of society. But, it is for a jury to determine if the defendant's conduct satisfies that expectation. Courts have expelled the argument that a prevailing custom absolutely defines the standard of care. That being said, custom may play a significant role in a judges' determination of the standard of care. [26]

Laws and regulations play less of a role than one might think in determining whether a defendant has been negligent. Court has not been willing to use statutory violations as the basis for a decision in which what occurred was not the harm that the statute was intended to prevent. Licensing standards have similarly not been used to determine negligence. For example, in a motor car accident involving a driver without a license, the criminal act of driving without a license does not automatically imply negligence. The two issues are separate. Similarly, compliance with licensing or mandated

[26] *Id.at 25*

operational safety requirements does not automatically mean that a party has satisfactorily fulfilled his or her obligations as a reasonable person and is thus immune from responsibility for negligence. So, a restaurant that has satisfied various health department inspections might nonetheless be liable for negligence in a litigation on account of food poisoning.[27]

There are five elements of a "cause of action" based on negligence by the defendant in case of cyber negligence:

- Duty
- Breach of Duty
- Cause in Fact
- Proximate Cause
- Damage

3.2.5. Threat and Impact of Cyber Negligence

Negligence is a person's fault without any involuntary or accidental action. Negligence has come forth as an important aspect of human safety and security. In the cyber space, negligence is a fairly common tort but with proper care and caution it is an avoidable wrong. For instance, in the cyber space, an e-commerce business owner has to employee great precaution and care in using and storing sensitive data of its customers, failing which it can lead to incidents of cyber negligence. Cyber negligence is thus arising as one of the most noticeable causes of security incidents. Another common example of negligence which is happening all around is giving electronic data to an unauthorized person. To gain a reasonable level of mitigation, internal awareness and training is very important to build the first level of awareness and this should be a continuing action, if the business wants some breathing space.

Sending sensitive information to an unauthorized person is one of the best examples of negligence. In the past, this seemed like an inevitable human error, but now that the security controls are in place, data leaks can be protected.

[27] What are the elements of Negligence? Available at https://www.findlaw.com/injury/accident-injury-law/proving-fault-what-is-negligence.html (last visited on June 19, 2021)

This technology has dramatically reduced user engagement and increased user control. These controls prevent employees from emailing documents to person accounts, sending them to any file sharing site, or copying them to a USB drive. Another aspect at present is on account of the growing culture of BYOD (Bring-Your-Own-Device) which has increased cyber risks, especially in the case of stolen devices. Even in such a situation, advanced technology can delete stored data by remote access on stolen devices. If regular and timely inspections and checks are carried out, these measures would definitely prove useful. [28]

Experienced employees, even the common user of a cell phone and a computer can also fall sufferer to negligence. Inadequate system configurations, bad patch management practices, and bad password management practices are some examples of skilled system and network administrators making unintentional mistakes. To protect their security infrastructure, organizations can put in place various security controls and put in place effective monitoring and compliance systems. [29]

Factors such as lack of awareness, inadequate education and lack of training can increase the risk of human error. Tools and techniques are available to greatly mitigate these risks. People use their smart phone and computer without knowing the risk factor however a hacker will always notice a person's carelessness which can lead to the commission of a cybercrime such as stealing personal data, identity theft, breach of privacy, etc. Some of the common instances of cyber negligence are as follows:

a) Falling for Phishing Attacks

Phishing is the fraudulent act to send an electronic communication pretending to be from a reputable source in order to obtain financial information, sensitive date, passwords, usernames, etc. The most common type of phishing attack occurs when an email containing malicious content is sent

[28] Negligence the number one cause leading cyber attacks, *available* at https://blog.eccouncil.org (last visited on March 02, 2020)
[29] *Ibid*

using a trusted source and these phishing emails focus on receiving private messages and confidential data of the user. As per the Verizon Data Breach Report, 2018, 96% of the time, emails serve as an attack vector, while 93% of breaches generates from phishing and pretexting.[30]

b) Bad Password Practices

In a survey conducted by Proofpoint–Wombat Security's 2018 User Risk Report advised that over 60% of respondents (among more than 6000 surveyed working professionals from the United States, the United Kingdom, France, Germany, Italy, and Australia) admitted that they do not use a password manager and are reusing passwords across various digital platforms. Here unsafe practice may compromise all of the accounts using the same login credentials. Poor password practices include sharing passwords with the third person, saving passwords on the same computer (particularly in plaintext format), using simple passwords, or not updating passwords on a regular basis. Indian users also have a terrible track record in this regard with more than 80% of users saving their passwords on smart phones and computers without updating their antivirus software. In India, maximum users do not use a genuine operating system (OS) on their computer and laptop rather purchase a pirated version of the OS in order to save some same. Such negligence can give occasion to cyber theft or a cyber attack to steal or corrupt our information and other sensitive data.

c) Incorrect Management of Privileged User Accounts

Sometimes highly privileged accounts can be mismanaged, especially by administrators and persons in the banking system. They are protected with inadequate security controls and in a number of cases are rarely updated. Such types of practices make admin accounts an easy target for cybercriminals. Once compromised, hackers can break secure networks to access sensitive data.

d) Unauthorized Users Having Access to Corporate and Common Devices

[30] *Id* at 28

As the earlier-mentioned Wombat Security's report, also recommends that 55% of working professionals give their device to their friends and family members, who access their employer-issued devices.[31] These unauthorized users of a digital device can get access to sensitive data as well as they can download malware accidentally. Common users also give their smart phone and laptop to strangers or to less known people without keeping in mind the fact that they may download or install unwanted malware or give access to an online perpetrator by mistake. Unauthorized use of mobile phones can give rise to the risk of danger to the owner of such a device. Nowadays, a number of softwares and apps relating to beauty, gaming, face changer are being used extensively and have led to incidents of image morphing, data privacy breach, identity theft, etc.

e) Misdelivery

In recent years, the healthcare industry has witnessed accidental disclosure of protected healthcare information. People sending an email containing health information to wrong recipients fall under the category of "misdelivery." This is one of the most significant errors to avoid. Users of digital devices give tremendous personal information to unknown or less known recipients like sending information regarding health history, sending data to an astrologer with genuine date of birth details, opening an email or WhatsApp attachment to fill out the personal information including financial information like account details, credit card or debit card details etc.

To avoid cyber negligence and keep oneself safe and secure, the best way is to improve the detection capabilities of the organization, the individual and the society at large. Identifying unusual spikes in the user's activity indicates a rise in incidents of negligence as well. While using proactive detection features with quick response strategies may reduce human error and the matter of negligence to a great extent, social awareness program, legal literacy and other

[31] White-papers/user-risk-report , *available at* https://www.proofpoint.com/us/resources/ (last visited on March 02,2020)

strategies can contribute significantly in this regard so that one is aware and conscience of human error. Aside from these tools, the human aspect must also remain in control as well.[32]

In the USA, California enacted a new law on cyber negligence titled The California Consumer Privacy Act, 2019. Companies had concern about their expanding potential liability. Companies fear that private rights of action are being created that will allow consumers to sue by alleging that the companies failed to protect their personal information. Attention must also be drawn in this regard to the rise in recent plaintiff victories in applying existing legal frameworks such as basic tort law to cyber cases.[33]

One such victory took place on January 28, 2019 when the U.S. District Court for the Northern District of Georgia announced a judgment in the Equifax Consolidated Consumer Class Action, allowing the consumers' negligence claims against Equifax to go forward. Judge Thrash decided that the consumers had enough alleged injuries resulting from the breach, guiding to the "unauthorized charges on their payment cards as a result of the data breach" as actual, concrete injuries that are legally cognizable under Georgia law. The Court denied Equifax's arguments that the consumer's injuries should be attributed to the hackers and could have been caused by data breaches at other companies. The court stated it allows businesses "to rely on other data breaches to defeat a causal connection would 'create a perverse incentive for companies: so long as sufficient data breaches take place, private companies will never be found liable." Critically, the Court observed that, given the foreseeable danger of a data breach, Equifax owed consumers an independent legal duty of care to take reasonable measures to safeguard their individual information in Equifax's custody. In doing so, the Court held that the doctrine of financial loss was not a bar to consumer recovery because Equifax was

[32] *Supra* note at 16, pg.75.
[33] The rise of cyber negligence claims plaintiffs find-receptive-judges by going back to basics *available* at www.dpwcyberblog.com2019/03/the-rise-of-cyber-negligence-claims-plaintiffs-find-receptive-judges-by-going-back-to-basics/(last visited on March 3, 2020)

indebted to an independent duty to protect personal information. Recently, courts had regularly ruled against these types of negligence claims in the meaning of cybercrimes.[34]

3.3. Cyber Privacy

With the Information and Communication Revolution (ICR) pacing fast to broaden its horizon, the internet has become the rapid growth means of communication through e-mails, chats, browsing, games, feedback, etc. There is increasing trust in computers concerning all facets of life. i.e., we trade and communicate with the help of computers and the internet, obtain many services such as medical advice, ticket reservation, ordering food, etc. on the internet. All this has changed the structure of society in a way that the computer today occupies a very important place in our lives. This leads to a cyber paradox; on the one hand, the computer and the internet have accorded extreme privacy and on the other hand, the same tool of technology allows the invasion of privacy. Today, the information superhighway is indeed not the safest place to be.

Privacy on the internet is a major concern nowadays. On August 24, 2017 the Hon'ble Supreme Court of India in the case of Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.[35] declared that a right to privacy is a fundamental right under Article 21 of the Constitution of India. In this case, the nine judges bench of the Apex Court declared that:

The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

The judgment is the outcome of a petition challenging the constitutional validity of the Indian biometric identity Aadhaar scheme. The judgment

---

[34]Vladimir Zwass, *International Journal of Electronic Commerce* , *available at:* https://books.google. co.in/ books? isbn=1591403561 (last visited on April 15, 2016).

[35] (2017) 10 SCC 1

observed clearly that the right to privacy as a fundamental right marks a watershed moment in the constitutional history of India.

This challenge came on account of the uncertainty on the nature and scope of privacy as a right in India. The government had taken steps to obtain and compile both demographic and biometric data of citizens. The primary justification for introducing Aadhaar was to secure government benefits reach the intended recipients. Following a speedy roll-out and expansion, this formed the largest biometric database in the world, with over 1.25 billion Indians registered. The government's push for Aadhaar has led to its universal acceptance as evidence of identity, and as a tool for restructuring and facilitating government services.[36]

3.3.1. Consumer Privacy

Well-developed legal framework on consumer privacy protection can be found in the United States of America, Europe, as well as under the guidelines of the OECD. Such laws are based on the following principles which are as follows:[37]

a) **Notice and Consent -** Before collecting data, the data subject should be provided: notice of what message is being collected and for what purpose and an opportunity to decide whether to accept the data collection and use. Data collection cannot continue unless the data subject has unambiguously given his consent (barring certain exceptions as envisaged under the law, as is the case in Europe).

b) **Use/Disclosure Limitation -** Data should be used only for the purpose for which it was collected and should not be used or disclosed in any way incompatible with those purposes.

[36] India's supreme court upholds right privacy fundamental right and its about time , *available* at www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time (last visited on March 02, 2020)

[37] Rodney D Rayder *Introduction to Internet Law and Policy* 314

c) **Retention Limitation -** Data should be kept in a form that permits identification of the data subject for no longer than is necessary for the purposes for which the data was collected.

d) **Accuracy -** The party collecting and storing data is obligated to ensure its accuracy and where needed, keep it up to date. Every reasonable action must be taken to ensure that data which is inaccurate or incomplete is corrected or deleted.

e) **Access -** a data subject should have access to data about himself, in order to verify its accuracy and to determine how it is being used

f) **Security -** those holding data about others must take steps to protect it and ensure its kept confidential

3.3.2. Privacy Protection against the Government.

The right to privacy is internationally recognised as a human right. Nevertheless, maximum Governments claim to have the authority to invade privacy through the following means:[38]

- Interception of conversations in the real-time
- Interception of traffic data (routing information) in real-time
- Access to data collected by service providers, including traffic data being stored for billing purposes
- Access to data stored by users

These means of access to communications and saved data must be narrowly described and subject to independent controls under strict standards. Real-time interception of communications should take place only with prior consent by a judge, issued under standards at least as strict as those for policy searches of individual homes.[39]

3.3.3. Indian Law Relating to Privacy

[38] State of privacy India, *available at* https://privacyinternational.org (last visited on May 14,2020)
[39] *Ibid*

Significantly, in India, there is no specific law governing data privacy. The Courts in India have not yet had the opportunity to look at privacy issues relating to the internet. Therefore, issues pertaining to privacy on the internet will, therefore, have to be drawn from cases that the Courts have actually dealt with.

The Constitution of India does not specify the fundamental right to privacy per se. However, the Supreme Court has held the right to privacy under the fundamental right speech and expression under Article 19 (1) (a) and the right to life and personal liberty under Article 21. In India, the right to privacy is thus an unenumerated right granted to the individual. In the Puttaswamy judgment, the Apex Court decided that the right to privacy is a fundamental right under article 21 of the Constitution.

Information Technology Act 2000 (will be discussed in detail under Chapter 5) gives some protection for violation of privacy. Recently the cabinet of the Indian Government recommended a Data Protection Bill in December 2019 taking the country a step closer to framing a privacy law. The bill states that personal data classified as confidential will only be stored or processed in India.

The personal data protection bill, drafted by a panel chaired by Justice B.N. Srikrishna, a former Supreme Court judge and presented to the government last year, is critical to the way businesses, including global top tech companies like Amazon, Facebook, Google and others which process, store and transfer data pertaining to Indian consumers.

3.3.4. Internet Privacy Risks

Digital privacy is the privacy and security level of personal data announced by the internet. This is privacy is a broad term that refers to a diversity of factors, technologies and techniques used to protect private and sensitive data, communications and preferences. Internet privacy and anonymity are paramount to users, primarily as e-commerce continues to gain traction. Privacy violations and risks are standard considerations for any website under digital development.[40]

Digital privacy is a matter of constant concern for any user planning to make an online purchase or sale or visit a social networking site or participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen by hackers or cybercriminals.[41]

The violence of online privacy is growing rapidly these days because people are continuously using the internet and internet connected devices, be it to update a WhatsApp status or to update one's daily routine on Facebook, Twitter or share stories on Instagram, etc. Therefore, on account of this constant use of the internet, the risks associated with internet privacy are also increasing. The following associated risks are as follows:

a) **Phishing:**
An internet hacking activity used to steal user security data, including username, password, bank account number, security PIN or credit card number.

b) **Pharming:**
An internet hacking activity used to redirect a legitimate website visitor to a different IP address.

c) **Spyware:**

An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.

d) **Malware**:

An application used to illegally damage online and offline computer users through spyware, trojans, and viruses.

[40] Major internet privacy issues and how to avoid them, *available* at https://securitytoday.com.aspx (last visited on May 14,2020)
[41] *Ibid*

e) Free WI-FI

A person feels quite elated coming across free wifi and begins to use it continuously for entertainment, to surf adult websites, to access social media, to order food through Swiggy or Zomato, to go online and shop, etc. Often, such free internet is offered as a ploy by hackers to watch and lure such persons by offering free coupons or exciting offers. Once such a person clicks on such an offer or coupon, they are redirected immediately and end up losing privacy, sensitive data, even financial details leading to financial losses.

3.3.5. New WhatsApp privacy policy, 2021 and their impact on users

In the year 2021, WhatsApp has started with new terms and conditions. if the users do not agree with the terms, they cannot access WhatsApp. It is time till 15th May to think about whether to accept the conditions. More than 200 crore users worldwide use WhatsApp. The researcher has discussed in detail the impact of these terms and conditions on users and consumers.

a. What is WhatsApp's new policy?

New terms and privacy policies have been updated on WhatsApp. It says that users will have to agree to these policies. It is coming into effect from May 15, 2021. After this date, it will be necessary to agree. If you do not agree, you will not be able to use the account. You can visit the help centre for this. The policy is now getting the option of Agree and not now.

It says that in order to operate our services, the content you upload, submit, store, send or receive to the WhatsApp app can make them use, reproduction, distribution and display anywhere.

b. Why did WhatsApp take such a decision?

After the policy is agreed upon, the WhatsApp app will be able to access the data of more than 200 crore users. That means they will also be able to share their data on other platforms. In the notification of the new policy, he has clearly written that the WhatsApp app will now share every information with your parent company, Facebook and Instagram. The WhatsApp app can also earn money by using its users ' data.

c. How will the policy affect the user?

It has been decided that if you run the WhatsApp app, these policies have to be agreed. That means you have to share your WhatsApp privacy with the company. That means the WhatsApp app will now keep a close watch on your data and your privacy is completely exhausted.

d. Ads to be determined by expenses

WhatsApp will track your bank name, amount and delivery location. This will also help facebook-Instagram know your financial transactions. The company will be profiling your transaction detail. That is, if you eat idli-dosa, you are not a rich man. When you go to Starbucks, you are rich. Then you will see advertisements of expensive trains.

e. IP address and location trace

WhatsApp has given the option that users can disable their location access. However, he has also said that the IP address and mobile number will be guessed when you go.

f. Status not safe either

WhatsApp will also read your status. The risk is if you write and tell which train to buy. So Facebook-Instagram will also read it and you'll see car, bike ads. Just like if you wrote and where you should go. Then there will be many tour ads on your social page.

g. Content will receive a presentation and analysis

WhatsApp will also give you the details of friends, groups, content, etc. In a way, the WhatsApp app will keep an eye on all your movements and analyse them. Facebook will show you shopping, product ads on this basis.

h. The call will also be monitore

Will the company know who you call how many WhatsApp calls? Which group are more active? What is the broadcast list? Photo-video forward will store more time on the server. He will know which content is becoming more forward. This information will be important at the time of tracking and election news. The WhatsApp app will also have access to the catalogue shared with the business account.

i. Should the policy be accepted?

The new policy is going to have a profound impact on user privacy. That means, as soon as you agree to the company's new policy, it will also give them rights to access your data. The problem is that the WhatsApp app needs to be agreed upon policy. The policy has to be accepted. If you do not agree, the WhatsApp account will have to be deleted.

j. What happened to the company's end-to-end encrypted policy?

The WhatsApp app claimed in its end-to-end encrypted policy that your messages, data, did not even have it. The company wrote in its policy that your privacy and security are at the top of us, so we have prepared the end-to-end encryption feature for you.

End-to-end encrypting protects your messages, photos, videos, voice messages, documents, status and calls and no one can misuse them. The end-to-end encryption feature ensures that messages and calls remain just between you and your contact. No one else, even WhatsApp, could not read, hear and see them.

3.3.6. Case Study on Cambridge Analytica and the Facebook 2019 Scandal: Violation of Cyber Privacy[42]

The researchers of Cambridge University claimed that by using a model developed by scientists using a combination of dimensional decrease strategy

[42] Facebook data privacy scandal a cheat sheet *available at* /www.techrepublic.com article/facebook-data-privacy-scandal-a-cheat-sheet/(last visited on March 7,2020)

and planning to infer data information about an individual it could "be used to automatically and accurately predict several sensitive private information, including nationality, sexuality, political beliefs, religion and happiness, personality, intelligence, happiness, addictive use, the divorce of parents, age and affinity".

The model according to the researchers was successful because of the similarity of certain properties. However, most people did not particularly like their characteristics. The Cambridge Scientists noted that "less than 5% of homosexual labelled users were directly related to gay groups," but "meet" Juicy Couture and Adam Lambert as "an indication of gay" whereas "WWE" and "being confused after waking" points to straight men. Other connections of this type are for instance "curly fries" indicates a high intelligence index, "sour sweets" indicates that "he does not smoke" and "Gene Wilder" indicates that the user's parents had not separated by age 21 years.

Facebook has more than a decade of incidents focused on inadequate and inefficient measures to protect data privacy. Although the severity of these individual cases varies, a series of repeated errors creates a bigger picture of common problems.

In 2005, MIT researchers built a manuscript that publicly retrieved information from more than 70,000 users in four schools however Facebook did not permit search engines to obtain profiles till September 2007.

In 2007, user activity on other websites was automatically added to Facebook's user profile as part of 'Beacon', one of Facebook's first attempts to monetize user profiles. For example, Beacon posted on Facebook the news feed for the titles of the videos that users rented from the Giant Blast Video, which violated the Video Privacy Act. A lawsuit has been filed in which Facebook paid $ 9.5 million to the Privacy and Security Fund as part of a settlement agreement.

In 2011, following an investigation by the FTC[43], the company approved a consent decree and promised to address concerns about tracking and sharing user data. The study was triggered by an event in December 2009 in which information that users believe was private was publicly shared, according to contemporary New York Times information.

In 2013, Facebook released information about an error that revealed personal information about six million accounts a year. If users recovered their personal Facebook account, this user would get the same action not only their own e-book but also the email addresses and phone numbers of their friends that others had stored in their laptops addresses. The data revealed by Facebook was not originally shared with Facebook by users, they were removed from the contact lists of other Facebook users who knew this person. This observable fact has since been described as “shadow profiles”.

The data privacy scandal by Cambridge Analytica began in February 2014. A series of reviews on the Turkopticon website a third-party review website for Amazon Mechanical Turk users - detailed a task directed by Aleksandr Kogan (American data scientist working in the Department of Psychology, Cambridge University) asking users to finish a survey in exchange for money. The survey directed users to add the “This is Your Digital Life” app to their Facebook account, which was against the terms of use of Mechanical Turk. One notice indicates that there were requests requiring that users “provide our app with access to your Facebook so that we can download some of your data - some demographics, your likes, your friends list and family information”.

On March 17, 2018, the matter was exposed by the Guardian and The New York Times, initially reporting that 50 million Facebook profiles were collected by Cambridge Analytica. The figure was later revised to indicate that the number was as high as 87 million. This exposure relied on the information provided by Christopher Wylie, a former SCL Elections employee and Global

[43] Federal Trade Commission (FTC) is a enforcement agency who enforces a variety of antitrust and consumer protection laws affecting virtually every area of commerce.

Science Research, author of this Orange Court. Wylie claimed the data from that program was sold to Cambridge Analytica, which used the data to develop 'psychological' profiles of users and target users with Trump ads, a statement that Cambridge Analytica denied.

On March 16, 2018, Facebook threatened the Guardian with charges of publishing the story, according to a tweet from Guardian journalist Carole Cadwalladr. Campbell Brown, a former CNN[44] reporter who is currently managing director of Facebook Information Partnership, said this was "not our wisest decision" and "If I were, I probably wouldn't have threatened to sue The Guardian". Similarly, Cambridge Analytica as well has threatened to sue The Guardian for libel.

On March 20, 2018, the FTC launched an investigation to investigate whether Facebook had violated the terms of the 2011 Rules of Investigation. In April 2018, reports indicated that Facebook authorized Zuckerberg and other top management to manage personal information on a platform that was not accessible to ordinary users. Zuckerberg's messages sent to other users were remotely erased from users' mailboxes, which the company said were part of corporate security measures following the 2014 Sony Pictures hack. Facebook subsequently announced its plans to make available to all its users the "unsend" feature and thus Zuckerberg would be unable to unsend messages until this feature is made available on Facebook. 10 months later, on February 6, 2019, the feature was added on Facebook. Public feature allows users to delete messages for up to 10 minutes after posting a message. In the disputes that led to this feature being added, it was reported that Zuckerberg removed messages months after they were sent.

On December 5, 2018, documents received in the probe of 'Six4Three' were issued by Parliament. Damian Collins, the MP who issued the order

[44]CNN (Cable News Network) is an American news-based pay television channel owned by AT & T's Warner Media. CNN was founded in 1980 by American media proprietor Ted Turner as a 24-hour cable news channel.Upon its launch in 1980, CNN was the first television channel to provide 24-hour news coverage and was the first all-news television channel in the United States

compelling the handover of the documents in November, six key points from the documents are as follows:

1. Facebook joined into white listing agreements with Lyft, Airbnb, Bumble, and Netflix, allowing those groups full access to friends' data after Graph API v1 was discontinued. According to Collins, "It is unclear" whether there was user consent for this, or how Facebook determined which companies should be white listed or not.
2. According to Collins, "the increase in revenue from major developers has been" one of the main drivers of the changes to the Facebook's Facebook platform. The idea of tying friends' data access to the financial value of the entrepreneur's communication with Facebook is a recurring feature in the documents".
3. The reciprocity of data between Facebook and developers has been a key issue in Platform v3, where Zuckerberg discussed contractor payment for friend lists. Internal discussion of changes to the Facebook Android app acknowledges that it was disputed to request permission to collect calls and text messages sent by the user, with the project manager speaking it was "pretty risky" to do from a public relations standpoint perspective.
4. Facebook used the data collected through Onavo, a VPN service purchased by the company in 2013, to investigate the use of smartphones. According to Collins, this happened "clearly without the users' knowledge" and was used by Facebook to determine "which business to acquire and who to treat as a threat".
5. Collins says that "records show that Facebook has taken an aggressive stance on apps, with the consequence that denying them access to data led to the failure of that business". Medical records specifically state that Facebook revoked API access[45] to the Vine Sharing Service.

[45] API access is the process of ensuring that calls with authenticated logins can enter APIs. An API gateway is the core of an API management solution. An example of API access is Google APIs. These APIs provide machine learning and analytics. They also allow access to user data when permission is given.

6. In a statement, Facebook stated that "Six4Three[46] has been tagging these documents since ancient times." Zuckerberg individually responded to a public announcement on Facebook, admitting that "like all organizations, we had great internal discussions and people came up with different ideas" and called the Facebook check "healthy compared to the many people who use our services" but said it should not "misrepresent our actions or incentives". The Facebook Photo API, created in 2018 revealed a vulnerability that uncovered $ 6.8 million personal photos of users. Image errors affected people using Facebook to connect to third-party services.

In December, 2018 The New York Times reported extraordinary data-sharing agreements that "exempted business partners from their usual privacy policies and named Bing search engines, Microsoft, Netflix, Spotify, Amazon and Yahoo" as partners in the report who would be able to access the data, including friend lists and private messages and claimed that despite public statements, this type of sharing had been terminated years earlier.

On January 17, 2019 Facebook has announced the removal of hundreds of pages and accounts operated by the Russian propaganda agency Sputnik, including reports published by politicians primarily from Eastern European countries.

On January 29, 2019 'The TechCrunch' report introduced Facebook Research, which pays users between the ages of 13 and 35 up to $ 20 a month to build a VPN application similar to Onavo, which allowed Facebook to collect almost all information about how the phone was used. On the iOS, it

[46] Six4Three is a tech company which produced a way to search for bikini pictures from your contacts on Facebook. After Facebook closed off access to data in 2014, the company sued Facebook for destroying that line of business, hoping to recover the money invested in the app.During discovery Six4Three obtained email and/or internal documents allegedly showing how much Facebook-founder Mark Zuckerberg knew about the privacy gaps in the Facebook partner API. This same API was abused by Cambridge Analytica to data mine information on tens of millions of US voters from a few hundred thousand users. Damian Collins, a UK MP investigating Cambridge Analytica, took interest in the documents and compelled their release in November 2018 by threatening the founder of Six4Three with imprisonment while he was in the UK on other business.

was distributed through Apple's development program, however Apple recalled it briefly from Facebook due to a dispute.

Initially, Facebook stated that less than 5% of people who opt in to this market research program were teenagers. Subsequently, the figure went up to 18 percent.

On February 7, 2019, the German Antitrust Authority has decided that a three-year-long investigation would require approval from Facebook before collecting non-Facebook data. Furthermore, by 20th February 2019, Facebook added a new location control to its Android app, allowing users to restrict background data collection when not in use.

On the same day, ZDNet announced that Microsoft Edge had a secret whitelist that allowed Facebook to run Adobe Flash and bypass the click policies that other sites rely on for Flash objects larger than 398x298 pixels. The whitelist was subsequently removed. On 6th March, 2019, Zuckerberg announced plans to restore encryption and privacy services in the coming years. As part of these changes, Facebook would match messaging between Facebook, Instagram and WhatsApp. Former Microsoft CEO Steven Sinofsky applauded the move and compared it to Microsoft's 2002 edition.

Dan Patterson, head of CNET and CBS News, told CBSN that Facebook could benefit from this consolidation if it were cheaper to operate and profit from users sending money via the messaging platform in a business model similar to Venmo .

By March 21, 2019, Facebook informed of a fault in security protection which caused hundreds of millions of passwords in plain text, exposing Facebook, Facebook Lite and Instagram users to severe privacy threat. Facebook said that these passwords were never exposed to the public at large and no evidence was found to prove that it had been abused by any employee within the company. Although the Facebook post does not provide specific information, former security journalist Brian Krebs reported that 200 to 600 million users were affected and that more than 20,000 Facebook employees had access.

However, on the March 22, 2019, Washington court ruled that Facebook was aware of the Cambridge Analytica scandal several months before its first official announcement in December 2015. Facebook said employees were aware of Cambridge Analytica rumours, but the allegations were related to “another incident”. Facebook avoided the main scandal and stubbornly claimed that the company did not mislead anyone in terms of the timing of the scandal.

Facebook sought to dismiss the case registered in Washington DC, as well as to seal a document filed in that case. On March 31, 2019, Facebook introduced a feature that explains why content is shown to users on their news feeds. On April 15, 2019, it has been revealed that Oculus, a Facebook-owned company, shipped VR internally etched headphones including texts such as “Big Brother is Watching”.

On April 18, 2019 Facebook posted “unintentional” email About 1.5 million mail contacts Consumer cropping for three years. Affected users were asked to provide email. Email addresses to confirm their identity.

On April 30, 2019 at a Facebook F8 contract conference, the company unveiled plans to review Messenger and reset Facebook to prioritize groups with the purpose as stated by Zuckerberg that “the future is a private matter”.

On May 9, 2019, in a statement to The New York Times, Facebook founder Chris Hughes[47] urged Facebook to be broken up by the government regulators. Hughes, who left the company in 2007, cited concerns that Zuckerberg surrounded people who did not challenge him. “We are a nation with a tradition of reigning in monopoly, no matter how quiet the leaders of these companies are. Mark’s power is unprecedented and un-American” as stated by Hughes.

Supporters of a Facebook break-up usually cite the unwinding of social media network purchases of Instagram and WhatsApp.

Zuckerberg dismissed Hughes appeal for a break-up of Facebook by stating that “if you care about democracy and elections, then you want a

[47] Hughes is one of four Facebook co-founders, who originally took on beta testing and feedback for the website, until leaving in 2007. Hughes is the first to call for Facebook to be broken up by regulators.

company like us to invest billions of dollars a year as we build it. A truly sophisticated tool to combat electoral interference”.

On July 18, 2019 the House Committee on Financial Services raised grave concern and expressed mistrust over Facebook’s cryptocurrency: Libra. They stated that there had been a serious failure in the pattern of keeping personal information and data private.

Subsequently, on 24th July, 2019 the FTC announced a $5 billion settlement to Facebook for privacy violations. Facebook agreed to conduct a review of its consumer privacy as part of the settlement. According to CNET, Sony had access to the friend data and Facebook was immediately restricted in this regard as a part of the settlement. Specifically, the FTC drew up a settlement with Aleksandr Kogan[48] and former Cambridge Analytica CEO Alexander Nix[49] “to limit how they conduct business in the future and require them to delete or destroy personal information they collected.” The FTC announced a lawsuit against Cambridge Analytica on the same day.

Also Netflix on 24 July, 2019 in order to expose the entire issue, realised a web series called ‘The Great Hack’. It is based on the story of Cambridge Analytica and tries to resonate the message amongst the viewers to avoid social media and live together with friends and family.

CBI registered case against Cambridge Analytica

The Central Bureau of Investigation (CBI) has registered a case on January 22, 2021, at the UK-based political consulting company Cambridge Analytics and Global Science Research Limited (GSRL). They are accused of

[48] Is a Senior Research Associate at Cambridge University and co-founder of Global Science Research, which created the data harvesting this is your digital life app. He worked as a researcher and consultant for Facebook in 2013 and 2015. Kogan also received Russian government grants and is an associate professor at St. Petersburg State University, though he claims this is an honorary role.

[49] was the CEO of Cambridge Analytica and a director of SCL Group. He was suspended following reports detailing a video in which Nix claimed the company "offered bribes to smear opponents as corrupt," and that it "campaigned secretly in elections... through front companies or using subcontractors."

stealing data from 5.62 lakh Indian Facebook users. The investigation into the case was going on from 2018.[50]

According to CBI, GSRL had wrongly shared data of about 5.62 lakh Facebook users in India with Cambridge Analytica. This data was later used to influence elections in India. In March 2018, several media platforms had made allegations of stealing Facebook data on Cambridge Analytics. He quoted former employees and documents of the company as saying that he had stolen data of more than 5 crores Facebook users. It also includes the personal information of users.[51] On April 3, 2018, Cambridge Analytics said it did not have Facebook data of Indians. Two days later, on April 5, Facebook told the Government of India that Cambridge Analytics has stolen Facebook data of about 562,455 Indians through the app.

If data theft on Cambridge Analytics and Global Science Research Limited is cleared, it may be processed under it (Amendment) Act 2008 and IT Act 2000. The Act says that theft of personal or confidential data or information from a system of a person, institution or organization is also a cyber crime. You have access to the data of an institution or organization and you use it without permission, then it will come under the purview of the offence.

3.4. Cryptocurrency and E-Commerce

Crypto means confidential Currency or digital currency. It is a currency whose identity of the transaction is hidden and its data is in a language that not everyone can understand. Only two people who are dealing with transactions know how many bitcoins were bought or sold. This term was first given by computer engineer Wei Dai in 1998.[52]

---

[50]Facebook Data Theft Case, *Available* on www.bhaskar.com, (last visited on March 9,2021)
[51] *Ibid*
[52] Blockchain Definition: What You Need to Know, *available at* www.Investopedia.com (last visited on June 8, 2021)

This currency on the computer's algorithm is only digitally present. That is, like a rupee or dollar, you cannot hold it in hand. It can be placed in the wallet, but not in the wallet that fits into your jeans pocket made of leather, in the digital wallet. Bitcoin, Ethereum, Ripple, Litecoin, Ciccoin are also similar currencies Bitcoin is the first cryptocurrency. In the early few years, its value gradually increased, but after 2015, it made it famous among investors worldwide.[53]

One particular thing is that the world is still unaware of who was the brain behind this virtual currency made in 2008 and launched in 2009. It is said that a person named Satoshi Nakamoto started Bitcoin. They don't know who they are, where they are, whether they are in the world today or not. The identity of bitcoin in the world is the only advantage of investors in staying confidential. It is notable that in 2019 when the founder of Cafe Coffee Day suddenly committed suicide, what was the impact on the company's shares? In two days, shares of coffee day enterprises fell 37 cents. In market capitalization, the company incurred a loss of Rs 600 crore. The price came at 123 rupees 25 paise per share.[54]

The Central Bank of India (Reserve Bank of India) is considering bringing its digital currency (Digital Currency, virtual currency) into the country. The RBI said that because of the rapidly changing scenario of the payment industry, the arrival of private digital tokens and increased expenditure related to the management of paper notes or coins, many central banks around the world are considering bringing in digital currency (CBDC). The RBI has also set up an inter-departmental committee to study the possibilities of the central bank's digital currency and to frame guidelines for the same.

[53] The Rise of Cryptocurrency in Ecommerce: What You Need to Know, *available at* https://swankyagency.com (last visited on June 8, 2021)
[54]Who Invented Bitcoin? the Alleged Identities of Its Creator, *available at* https://www.businessinsider.com (last visited on June 8, 2021)

CBDC is a legal currency and digitally the central bank's liability is available as sovereign currency. It is recorded in the bank's balance sheet. It is an electronic form of currency that can be converted or exchanged in cash issued by RBI. These benefits will be that if digital currency is in circulation, money transactions and transaction methods can change. This will curb black money. The committee says digital currency will make it easier to adhere to the monetary policy. It should use Digital Laser Technology (DLT). DLT will make it easier to detect transactions abroad. In India, the circulation of cryptocurrencies has increased rapidly, but there is no law or guidelines to regulate cryptocurrency in the country. In 2018, RBI issued a circular on cryptocurrencies. The RBI had prohibited all financial institutions from providing cryptocurrency-related services. But after the RBI ban, The Supreme Court had dismissed the ban imposed by RBI last year. Cryptocurrencies are being traded in India after the Supreme Court ruling.[55]

In budget 2021 the government of India is preparing to ban cryptocurrencies like Bitcoin, Ether. For this, the government is going to introduce the cryptocurrency and regulation of official digital currency Bill-2021 in the forthcoming budget session.

E-commerce may be successful with the current fiat-based payments system in place, but virtual currencies can add a new dynamic to the fold. With increased convenience for consumers, an increase in cryptocurrency ownership, perpetually improving blockchain technology, and the reduced cost of circumventing intermediaries, virtual currencies can open a new door for e-commerce to extend its growth to its fullest potential.[56]

Cryptocurrencies provide greater security to users because of their near immutable nature and a lower cost to the consumer and merchant. Other benefits include full transaction traceability, full ownership of assets without

---

[55] *Id.* at 40.
[56]Crypto and blockchain cut the clutter for e-commerce *available* at: https://www.ecommercenewsfeed.com/general/2020/crypto-and-blockchain-cut-the-clutter-for-e-commerce (last visited on June 19, 2021)

intermediary institutions, privacy, and integrity of payments. Consumers around the world are picking up on these benefits and gradually more are joining the fray.[57] The inevitably increasing use of cryptocurrency, even if not to supplant fiat currency, can help hurdle old e-commerce obstacles. Payment transactions in traditional forms, like credit, debit, or other payment platforms that use fiat currency require intermediary companies to transfer payment between two parties.[58]

The rise of digital wallets is making way for more convenient and instant payment systems, and as a result, it is changing the way of conduct business and consumers tendency. The invention of cryptocurrency has changed the currency flow system for merchants and consumers. NO credit card, no debit card or UPI id, now all are the traditional mode of payment. cryptocurrency is going to replace all traditional payment systems.

Both centred around tech, it would be fair to assume that cryptocurrency and ecommerce have the potential to complement each other quite nicely – and, in a few cases, they already are. Cryptocurrencies, particularly Bitcoin, are already infiltrating the eCommerce industry, offering an innovative, viable and streamlined digital solution for many existing blockers. With the ability to appease consumer demand for immediacy and security, while expanding market share for retailers, cryptocurrencies could prove extremely beneficial for the eCommerce industry if adopted efficiently. More and more companies have grown to understand these benefits, leading to a surge in consumer attention, and it may not be long before we start to see the commercial use of cryptocurrency as standard.[59]

Cryptocurruncy definitely is a stirring new platform that can be used for currency. Today people are investing in this basic form of cryptocurrency.

---

[57] *Supra* note at 8, pg 231

[58] Crypto and blockchain cut the clutter for e-commerce"*available* at: www.paymentssource.com (last visi ted on 14 March 2021)

[59] The future of cryptocurrency in the e ommerce industry, *available* at: globalbankingandfinance.com https://www.google.com/search?q=The+future+of+cryptocurrency+in+the+e+ommerce+industry%2C +availablelast visited on Feb.21, 2021)

Bitcoin has seen rapid growth, falling and rising. Due to the risk profile and inadequate access to available payment gateways such as PayPal, banks and other third-party payments, a large part of the global population remains excluded from participating and enjoying the benefits of e-commerce. With the Bitcoin wallet, shoppers can easily avoid listing fees when buying products abroad. Fiat money transferred to e- currency can be transferred to any corner of the world without control.[60]

As Bitcoin wallets are entirely digital in nature, they allow users to save and return multiple copies of the same wallet. This allows you to receive full user data in case of users lose their wallets. Also for high-security reasons, a Bitcoin wallet is only accessible with the user's private key.[61]

All mobile and other devices Platforms like Android and iOS, support cryptocurrency business. The amalgamation of blockchain application technology and e-commerce has imprecise the way we understand and use the various e-commerce platforms accessible today.

With the advent of the internet, it has become easy for anyone to collect and use private information from individuals. Small, scattered and unimportant pieces of data have now become a powerful set of data that can be misused by businesses or by anti-social elements. This has led to many countries putting in place privacy legislations. However despite such initiative, it is becoming extremely difficult for persons to hide themselves in today’s digital age. It is a matter to think about that how in the present day and age, the internet is always with us and is always looking for us.

3.5. Cybercrime

With the development of new mediums of communication, business and societal activities, the growth of varied kinds of crimes was inevitable. Computers with the aid of the internet have today become the most dominant

[60] The Impact of the Bitcoin Revolution on ecommerce Industry, *available* at: www.digitaldoughnut.com https://www.digitaldoughnut.com/articles/2018/february/the-impact-of-bitcoin-revolution-over-ecommerce (last visited on June 19, 2021)
[61] *Ibid*

medium of communication, information, commerce and entertainment. The internet is at one moment a shopping mall, the next moment it could become a library, a university, newspaper, television, movie theatre, post office, courier service or even an extension of the government or business. It is like life in the real world being extended and carried on in another medium that cuts across boundaries, space, time, nationality, citizenship, jurisdiction, sex, sexual orientation and age. The internet, with all the benefits of anonymity, reliability, and convenience has become an appropriate breeding place for persons interested in making use of it for illegal gainful purposes, either monetary or otherwise.[62]

3.5.1. Types of Cybercrimes

Cybercrimes can take numerous forms. Here we look at several types of activities that constitute cybercrimes which includes cyber stalking, cyber theft, hacking activities, etc. Consumers are being cheated through different kinds of cybercrimes and it is increasing day by day.

The smartphone and laptop revolution has increased the e-commerce transactions and also the associated risk of cyber-crimes. The customer often lacks the basic awareness and the comparatively less stringent rules make India a favourable target for cybercriminals committing offences such as theft, phishing, spam, etc.

In the year 2018, approximately 27,250 cases of cybercrime were reported across India. This was an increase of more than 121 percent as compared to a number of cases reported in 2016. However, the real numbers could have been under-reported through the years due to a lack of cybercrime awareness or mechanisms to classify them. Recent government initiatives such as a dedicated online portal to report cybercrimes could be the reason for a sudden spike in a number of crimes from 2017 onwards.[63]

[62] S.K. Verma And Raman Mittal *Legal Dimensions of Cyberspace*, 228 (Indian Law Institute, New Delhi, 2004)

[63] Cyber crime in India, *available* at: https://www.statista.com/topics/5054/cyber-crime-in-india/ (last visited on March 05, 2020)

Data published by the National Crime Record Bureau (NCRB) on October 2017 provides that during 2017, 56% of cyber-crime cases registered were pertaining to cyber-fraud (12,213 out of 21,796 cases), sexual exploitation accounting for 6.7% (1,460 cases) and cybercrime causing disrepute accounting for 4.6% (1,002 cases).[64]

The American Bar Association defines computer crime as any act that is directed against computers and computer parts, that uses computers as instruments of crime, or that involves computers and constitutes abuse. A variety of different types of crimes can be committed with or against computers, including the cybercrimes discussed in the next section.

Many computer crimes fall into the broad category of financial crimes. Computer networks provide opportunities for employees and others to commit crimes that can involve serious economic losses. The dependence of businesses on computer operations has left firms vulnerable to sabotage, fraud, embezzlement, and the theft of proprietary data, such as trade secrets or other intellectual property. For example, employees of the accounting and computer departments can transfer monies among accounts with little effort and often with less risk than that involved in transactions evidenced by paperwork. The potential for crime in the area of financial transactions is great; most monetary losses from cybercrimes are suffered in this area.[65]

The theft of computer equipment and the theft of goods with the aid of computers (such as by manipulating inventory records to disguise the theft of goods) are subject to the same criminal and tort laws as thefts of other physical property. In many jurisdictions, the unauthorized use of computer data or services is considered larceny. Other computer crimes include vandalism and destructive programming. A knowledgeable individual, such as an angry employee whose job has just been terminated, can do a considerable amount of damage to computer data and files. Destructive programming in the form of

---

[64] Cybercrime ncrb-2017, *available* at: https://www.medianama.com // (last visited on March 05, 2018)
[65] Roger Leroy and Gaylord A. Jentz *Law for E-Commerce*, 96 (West Thomson Learnig USA 2002)

viruses, as mentioned earlier, presents an ongoing problem for businesspersons and other computer users today.[66]In the following pages, a few common cybercrimes have been discussed. Wherever possible, not only the meaning and scope of the crime but also its coverage under the Indian Information Technology Act, 2000 (hereinafter referred as the IT Act), Indian Penal Code 1860 and other criminal legislations have been discussed.

3.5.2. CYBER THEFT

In cyberspace, thieves are not subject to the physical limitations of the "real" world. A thief can steal data stored in a networked computer with dial-in access from anywhere on the globe. Only the speed of the connection and the thief's computer equipment limit the quantity of data that can be stolen.

a) Identity Theft

Identity theft involves obtaining legal information of a person that reflects his or her identity for economic purposes. This is a common form of cyber theft. Identity theft can be stolen even if the deceased is alive or dead. Formulating a fake account or false presentation by formulating multiple email ids has become so simple that resulted in the commission of fraud to collect any information that can be used by cybercriminals to take over the victim's identity to act infinite crimes.

Today advances in technology have made things much easier at the same time it is much harder to a person on account of the anonymity and privacy provided on the internet and online transactions. The internet engages primarily in virtual identities and therefore it is an arduous task to identify the true identity of the person on the other side. There are various techniques through which data theft could be committed and personal information could be procured from electronic devices. These are as follows: -

i) Hacking

[66] David L, and Andra , *et*.al., Computer *Crime: An Emerging Challenge: An Emerging Challenge for Law Enforcement, Cybercrime and Security*, 1.5-3 to 1.5-4 (1998),

Unscrupulously breaking into the information contained in any other digital system by another person is called hacking and the perpetrator is known as the hacker. Section 66 related to the offence of illegal access to the computer resource explains it as:

"Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking."

The offence of hacking is a breach of one's fundamental right to privacy as granted by the Constitution. Often, the offence of hacking involves the introduction of viruses or worms like malware, spyware installed in any computer or other devices, by this method cybercriminals steal the personal information and other sensitive data on the device. Hackers divert data from one computer system by decrypting it to the hacker who after receiving the information either uses it themselves or provokes others to act illegally by using such information.[67]

ii) Hacking and Cyber Terrorism

Hackers who break into computers without authorization commit cyber theft. Often, their principal aim is to prove how smart they are by gaining access to others' password-protected computers and causing random data errors or making unpaid-for telephone calls. Such crimes should not be taken lightly, but from a larger perspective, they might be considered the equivalent to a new-tech car theft.

Cyber terrorists, however, are hackers who aim not to gain attention but rather try to go undetected in order to exploit computers for a more serious impact. Just as a "real" terrorist might explode a bomb to shut down an embassy, a cyber terrorist might explode a "logic bomb" to shut down a central computer. Other goals might include a wholesale theft of data, such as a

[67]Cyber theft - A serious concern in India, *available* at: www.lexology.com/library/detail.aspx?g=4af6c044-dc77-4b1a-9288-986395eff8d1 (last visited on March 26, 2020)

merchant's customer files, or the monitoring of a computer to discover a business firm's plans and transactions. A cyber terrorist might want to insert false codes or data. For example, the processing control system of a food manufacturer could be changed to alter the levels of ingredients so that consumers of the food would become ill.[68]

b) Phishing-

Phishing is the method of using fake email-ids or messages containing viruses thereby affecting websites. By phishing, the hackers provoke the user to use infected websites and urge people to insert their personal information such as login details, account information, financial details, etc. Hackers make a fake URL which looks like the original URL and use the same colour and diagrams like the original so that the user trusts the URL and steps into their trap.

c) E-Mail/SMS Spoofing.

The E-Mail/SMS Spoofing is one of the commonest form of online fraud nowadays. It initially starts with an SMS spoofing through a mobile number or email message. It presents its origin to be different from where it actually originated. In case of SMS spoofing the sender's mobile number is hidden and replaced with an alphanumeric text. In case of email or SMS spoofing, the cybercriminal has the intention to steal the identification of another person.

d) Cloning of ATM and Debit cards (Skimming)

Today the act of skimming is a very easy task for cybercriminals. A lot of skimming crimes are happening daily, where often one may read in a newspaper as to how the ATM card was cloned and thereafter misused. The cybercriminals make illegal use of the ATM debit and credit cards to withdraw money from the bank accounts of the person. Cloning employs an electronic device to scan the card, so it does not require the physical card to be stolen. An

[68] Roger LeRoy Mille, *law for e commerce* 75 (,west Thomson learning, page, 2002)

employee would use a portable reader to scan the card prior to inserting it into a credit card terminal. This allows the information on a magnetic stripe card, which is typically encrypted during the transaction process, to be recorded in the device memory.

Once the information is recorded it can be transferred in the magnetic stripe of a new card or can be used to overwrite data on an already stolen credit card. For cards that use an ATM personal identification number (PIN) number in addition to a magnetic strip, like debit cards, the PIN would need to be inspected and recorded. [69]

Cyber thieves put the skimmer on the ATM card swiping device. However, only a skimmer is not enough. The crooks trying to deceive the people, either place a camera inside the ATM or hack the bank camera to get to know the ATM pin of the card user. Once the ATM pin is recorded and the card details are stored on the skimmer, the thieves use it to purchase things online or create cloned cards.[70]

Skimming is relatively one of the easiest and most commonly used method to clone cards. Recently the government has changed all ATM cards and released micro chip-enabled ATM cards for securing credit and debit cards. In 2020, the government also launched without the ATM card withdrawal of cash system through e-wallets and ATMs like SBI Yono, Canara bank cardless cash system, etc. user awareness is the best way to avoid fake calls and cloning.

e) Vishing

Vishing relates to the act of a cyber-criminal calling the victim by posing to be a bank representative or call center employee, thereby fooling them to disclose crucial information about their personal identity. Vishing is an OTP (One Time Password) theft offence that one may come across often, while

[69]Industry banking finance banking atm skimming, *available at* https://economictimes.indiatimes.com/industry/banking/finance/banking/atm-skimming (last visited on March 05, 2020)
[70] *Ibid*

going through the newspaper. It gives hackers an opportunity to make the victim undertake a transaction and share the OTP in a very easy manner.

OTP theft involves a person calling posing as a bank employee, ostensibly to update or renew credit/debit cards of those receiving the calls. The unsuspecting victim provides the card number and CVV, secure in the knowledge that any person would still need the OTP to carry out any transaction. The scamster then says the victim will receive an SMS, which would have to be sent back to the sender.

Mode of Vishing:

i. **Case number one**

   You picked a call, The caller gained the confidence of the person by getting the name and address correctly. The person then inquired whether he had recently bought or changed a new credit card and asked for some information for some verification purposes.

ii. **Case number two**

   You picked a call, the caller tells you sir/ma’am your ATM/credit card is going to expire and you may face financial loss, you are our loyal customer so kindly verify your account by clicking on a link or sending OTP.

iii. **Case number three**

   You picked a call, the caller is a girl and emotionally tells you Bhaiya/ Friend my and your number are same only one digit difference and I am filling online form today is last day, by mistake the OTP has been sent on your number, so please try to understand me this is question of my carrier, please share the OTP.

iv. **Case number four**

   You picked a call, the caller tells you that he is a police officer and warn you that your name was traced in that case so you may be arrested. However, if you are innocent provide identity and other details.

v. Case number five

The caller tells you that your id number and address and would say that your mobile number is going to be blocked on account of a banking security risk so kindly verify your number and provide KYC.

f) Fake Web Link (Web Jacking)

Web jacking originates from the term “hijacking”. Web jacking signifies that the hacker gets control of a website fraudulently. Hackers can change the content of the genuine site or also redirect the user to another fake similar looking URL controlled by him. The originator of the website no longer has command over the website and the attacker may use the website for his own selfish interests. Matters have been reported where the attacker has asked for a ransom and even posted obscene material on the site.

The web jacking system attack may be used to create a clone of the website, and present the victim with the new link stating that the site has moved. Unlike usual phishing methods, when you hover your cursor over the link given, the URL presented will be the original one and not the attacker’s site. But when users click on the given new link, it opens and is quickly replaced with the malicious web server. The name on the address bar shall be slightly different from the original website that can trick the user into thinking it’s a legitimate site. For example, “Gmail” may direct you to “gmai1”. Notice the one in place of ‘L’. It can be easily viewed.[71]

g) Denial of Service

A “denial of service” attack is identified by a specific attempt by the attackers to prevent legitimate users of a service from using this service. Examples include:

- To “saturate” a network, thus avoiding legitimate network traffic
- To interrupt connections between two machines, thus avoiding access to a service

[71]Fast track to cyber crime the-12 types of cybercrime, *available* at: www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html (last visited on March 05,2020)

- To prevent a specific person from accessing a service

In what has been described as the most devastating attack on the World Wide Web in internet history, a teenager named “Mafia boy” who on the 2nd of February 2000, managed to deny legitimate users the services of Yahoo.com by conducting an encyclopedia volume of electronic information every second. Using multiple university computers as “zombies”, he was able to attack the website from multiple virtual locations.

Denial of service attacks can significantly disable the computer or the network service. Depending on the nature of the business, this can effectively deactivate an organization. The term can be applied to any situation in which an attacker tries to avoid the use or delivery of a valuable resource to its target audience or client. It can be implemented by several methods, physically and digitally. For example, an attacker can deny access to telephone systems if he cuts the most important telecommunications cable that supplies a building, repeatedly calls all available telephone lines or breaks the switch that manages the exchange.[72]

Section 43(f) of the IT Act particularly provides for penalty if anyone is found guilty of causing denial of access. The sub-section provides that if any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means, he shall be responsible for the payment of damages for compensation not exceeding one million rupees to the person concerned. Therefore, any act resulting in denial of access would be covered by sub-section (f) of section 43 of the IT Act.

3.6. Cyber pornography

Generally speaking, cyber pornography refers to the stimulation of

[72] What is a denial of service attack (dos) *available* at https://www.paloaltonetworks.com (last visited on March 05,2020)

sexual activity or other erotic activities via the internet. This would include pornographic websites, pornographic magazines produced using computers to publish and print material, and the internet to download and transmit pornographic images, photos, writings, etc. In recent times, there have been countless cases of promotion of pornography through the use of the computer. Information technology has greatly facilitated the creation and distribution of pornographic material on the internet. These documents can be sent to everyone in seconds. Geographic restrictions which, up to now, have to some extent prevented foreign publications from entering local territory have also disappeared.[73]

The causes of growth in cyber pornography have been many and varied. Primary among them is the ease with which one can access pornographic stock online and its anonymity. People can quickly view thousands of pornographic images, day and night, in the privacy of their own home. The internet has reduced restraints of shame that comes with purchasing pornographic materials or the embarrassment of being caught with it. What has been most disturbing is the increase in child pornography. Child pornography is separate from other pornography, and consequently receives more powerful legal treatment. It is distinguished as a matter of child abuse. In its production and/or in the way it is used by paedophiles to desensitise their victims. The development of the internet has contributed child pornographers with a distribution vehicle that is observed to be relatively unknown.

In a significant development in protecting children from online pornography, the Bombay High Court Committee on Protecting Children from Online Pornography[74] gave its recommendations through its report dated 30.01.2002. The Committee was established pursuant to a letter sent to the

---

[73] S.k. verma and Raman Mittal(eds.) *legal dimention of cyberspace* 238 (Indian Law Institute 2004)

[74] The High Court Committee comprised of the Deputy Commissioner of Police the Chairman and Managing Director of VSNL, Vijay Mukhi or another authorised representative of the IUAI, S.K.Nair, Advocate, and Gautam Patel, Advocate. The Chairman and Managing Director of VSNL was represented by Dr. Sourav Dutta, the Deputy General Manager (Systems) of VSNL. The High Court order also directed that one authorised representative of the Internet Service Providers Association of India (ISPAI) and either the first petitioner, Jayesh Thakker or, in his absence, the second petitioner, Sunil Thacker, would be Special Invitees to assist the Committee. The ISPAI was represented by Brig. TM Sreedharan accompanied by Sudhir Gosar, a technical expert.

Hon'ble Chief Justice of the Bombay High Court complaining about the proliferation of pornographic sites on the internet. The letter was taken up as a suo motu writ petition. The internet Users Association of India (IUAI) was permitted to intervene in the matter. On September 28, 2001, a Division Bench of the High Court passed an order to appoint a Committee to suggest and recommend ways, measures, and means to protect minors from access to pornographic and obscene material and other related things on the internet. Based on the terms of reference contained in the high court order, the issues before the Committee resolved themselves into two broad categories: Regulatory and Educational. As regards the latter, it deals with increasing awareness among internet users, generally, through defined vehicles such as e-mail newsletters, online (website) content, hotlines and help desks.[75]

The regulatory issues and recommendations covered mostly the service providers. It includes cyber cafes, internet service providers (ISPs) and online portals that provide communication services. The Committee was of the view that it was inherently impossible or, at the very least, impractical to evolve a common set of regulations governing all classes of service providers. Every service provider has its unique combination of techno-economic capabilities and limitations. For example, online portals[76] that provide communication platforms and solutions (e-mail, messaging and chat) cannot assume the same liabilities as an Internet Service Provider, which provides access to the internet and, through, to all of its protocols, including those provided by online portals. The Committee made the following recommendations to protect children from pornographic sites on the internet:

1. Blocking of sites
2. Preventing minors from accessing unsuitable material from Cyber Cafes

[75] Cyber cafes under ITA 2008, *available a*t: *www.naavi.org* (last visited on March 05,2020)
[76] *Id.* at 47.

3. Preventing the publication or propagation of pornography from Cyber Cafes

The problem of cyber pornography has been dealt with in section 67 of the IT Act where the publishing of information which is obscene in electronic form has been made an offence. The section gives that any material which is published, or transmitted or caused to be published in the electronic form shall be an offence in the following circumstances:[77]

a. the material so published or transmitted is lascivious;
b. the material appeals to the prurient interest;
c. if the effect of the material is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

If someone is found committing a crime under section 67, he shall be punished with the first term of imprisonment in one of the descriptions for a period which may be extended to five years and with fine which can be extended to one lakh rupee and in the case of a second conviction or a subsequent conviction with imprisonment of any of the descriptions for a period of up to ten years and also with a fine of up to two lakh rupees. Note that the obscenity test in section 67 is the same as that in section 292 of the IPC which deals with the sale of obscene books, etc. Other provisions related to the subject are the Act on the Indecent Representation of Women, 1986 and the Young Persons (Harmful Publications) Act 1956. People who engage in cyber pornography accessible to people under the age of twenty can also be prosecuted under section 293 of the IPC.[78]

---

[77] S.k. verma and Raman Mittal(eds.) *legal dimension of cyberspace* 240 (Indian Law Institute 2004)
[78] Indian Penal Code, 1860, S. 293: Sale, etc. of obscene objects to young persons. - Whoever sells, lets to hire, distributes, exhibits or circulates to any person under the age of twenty years any such obscene object as is referred to in the last preceding section, or offers or attempts so to do, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to seven years, and also with fine which may extend to five thousand rupees.

3.7. Misleading Advertisement

Misleading advertisement is an advertisement which is factually incorrect or in a manner deceptive while conveying the information about the product. Misleading advertisement can also be done in respect of determining whether any advertisement is misleading through ingredients of the product or by tag lines of the product such as “I am a complan boy” or the line “effect as much as six times whiter, as a woman becomes fairer she is seen happier.” So, misleading advertisement tend to mislead consumers. The brands circulates misleading advertisement, which state in an ambiguous note and lacks actual facts. The problem of such an advertisement is that the consequences are felt only after the product is bought. Advertisements can be misleading if they contain false statements of fact, conceal or leave out important facts, include or imply a promise to do something without the intention of carrying it out, or create a false impression, even if everything stated may be literally true. In India, many consumers treat celebrities like a superhero or God and thus trust blindly whatever they show, claim or endorse.[79]

3.7.1. Significant Aspects of Misleading Advertisement

There are a number of problems that have affected the marketing scene on account of deceptive advertising. The first of them is advertising made to children. These advertisements ads are created in such a way that they target individuals who do not have the ability to differentiate fictional facts from the truth and therefore such ads are arguably misleading.

Sexual appeal is explicitly used to sell all kinds of things. It is used to get the consumers’ attention. It is used where it is not even appropriate for the product or service being used. The ladies are shown as decorative or sexually provocative objects, even for products where women are not required.

Usually, the consumer is attracted to a retail outlet by an advertisement for a low cost branded item, however, they are unaware of the hidden price

[79] *Available* at: https://www.mygov.in/frontendgeneral/pdf/brief-on-misleading-advertisement.pdf (last visited on March 05, 2020)

which are never shown in the advertisement and is sold at a higher-price version. Once the consumer enters the store, he/she is compelled by the sales girls to purchase another more expensive item. In such stores, one finds a handful of out-dated products on the discount so advertised and other fresh and better products at full price. If consumer purchased goods the shop offers further coupons are issued to the customer to lure him to shop more worth a fixed amount in order to avail the coupon or receive a further gift or prize.

Fake and misleading ads, in fact, violate the right of choice, the right to be informed and protected against unsafe goods and services, as well as unfair business practices.[80]

Outdated laws, poor compliance with laws are the main reasons for the prevalence of bad advertising. The need of the time is to put in place better laws, periodic updating of laws, better enforcement of laws, deterrent measures and ensure regular monitoring of such advertisements and announcements by the particular authorities.[81]

Misleading advertisements is not only affecting the young generation but also interferes in the various aspects of social and religious life of society. For instance, if you switch on even a news channel one may find a religious guru or a 'baba' being questioned by the anchor about the attainment of happiness and money by an individual, who then in return tries to educate the people about his magical treatment and lastly advertises himself by providing his contact number and address and advises to call for happiness. Another example can be misleading advertisement and false claims made about organic medicines being broadcasted through TV channels where such babas and doctors claim to treat even the most impossible diseases such as cancer, old age bone problem and much more with their products.

3.7.2. Existing Legislations to regulate misleading advertisement:-

- The Drugs and Cosmetics Act, 1940

---

[80] *Id.* at 67.

[81] Brief on Misleading Advertisements, *available* at: www.mygov.in/frontendgeneral/pdf/brief-on-misleading-advertisement.pdf (last visited on March 05, 2020)

- The Drugs and Magic Remedies (Objectionable Advertisements) Act, 1955
- Food Safety and Standards Act, 2006
- The Cigarettes and other Tobacco Products (Prohibition of Advertisement and Regulation of Trade and Commerce, Production, Supply, and Distribution) Act, 2003
- Consumer Protection Act, 2019

Moreover, the advertisements aired on private satellite TV channels are regulated under the Advertising Code prescribed in rules framed under Cable Television Network (Regulation) Acts 1995. The misleading advertisements in print media, which are violation of 'Norms of Journalistic Conducts' are being adjudicated by the Press Council of India under Section 14 of the Press council Act 1978. The Food Safety and Standards Authority also provides for penal action against misleading advertisements pertaining to food products.[82]

3.8. Conclusion

Cybercrime has its roots worldwide and severely affects global business directly or indirectly. The government, organizations are taking measures to prevent the consumer and develop electronic commerce free of cybercrimes. The consumer must be aware of and cooperate in the prevention of cybercrimes.

In India a vast diversity of consumers live here, most of whom are technically unsound, while some consumers are illiterate and some have knowledge of computers but fail to keep up and stay updated with the technological developments. Therefore, there is a dire need to develop an awareness program according to the status of the consumer.

There is a wide legal framework in India to stop such misleading advertisements but all fall short of fulfilling this task on account of the lack of proper implementation of these laws in India. No such active legal authority

[82] Brief on Misleading Advertisements, *available* at: https://www.mygov.in/frontendgeneral/pdf/brief-on-misleading-advertisement.pdf (last visited on March 05, 2020)

has been established which focuses on effective, efficient and immediate action against such companies, e-commerce business, marketplaces, etc.

Due to the tardy legal procedure and the existing corruption, it has been rarely seen that any accused gets imprisonment for food adulteration or misleading advertisement.

The consumer should also take extra precaution at the time of shopping online or while undertaking an online transaction or even at the time of swapping an ATM/credit cards in a shop. Approximately 70% of consumers are cheated by hackers, skimmers because they do not take precautions at the time of online shopping.

The issue of privacy on the internet is of concern to many people. Many coalitions have been formed to monitor and disseminate information regarding privacy issues on the internet and to proactively lobby for greater privacy measures. So what information is to be kept about a visitor online? The answer depends on how much information the visitor divulges about him/herself and how he/she configures the web browser preferences. Cookies were designed to allow web servers to operate more efficiently, provide a better response time to repeat visitors to their sites, and more accurately track how many different users (as opposed to repeat visitors) visit a site. The use of cookies, however, has become a very controversial topic by privacy groups preferring to have no information about web browsing activities should be kept by the websites visited.

The internet and e-commerce offers unlimited possibilities and opportunities to businesses of all sizes as well as freedom to consumers. However, these benefits are not reaped without risks, to both merchants and consumers. Unfortunately, the fast-paced evolution and exponential growth rates of electronic websites have enticed many enterprises to embrace technology without fully understanding the ramifications and control issues involved. Furthermore, some consumers eager to “point and click” to purchase their desired products have found themselves vulnerable to unsafe and unsecured systems. Moreover, media coverage, and sometimes, media hype, about these consumer risks have caused many potential consumers to be leery about electronic transactions and to refrain from engaging in such activities.

The next chapter undertakes the study of information and communication technologies (ICTs), its impact on global economic processes, including international trade and e-commerce. Furthermore, the next chapter provides an overview of the trends and indicators on the use of ICTs in this regard. It also examines it in terms of the economy, development, growth and trade, particularly in e-commerce. It also fleshes out the existing international legal gamut on e-commerce and e-commerce related aspects.

CHAPTER - 4

INTERNATIONAL FRAMEWORK OF E-COMMERCE

CHAPTER - 4
INTERNATIONAL FRAMEWORK OF E-COMMERCE

The preceding chapter explores the various forms and kinds of risks faced by consumers during electronic business transactions. The chapter analysed the factors leading to rapid growth and advancements in corporate information systems and associating the same with the increased risk which could be faced by such consumers on this account. Therefore, the chapter discussed the overview of the present legal regime, issues and challenges before it vis-à-vis new technology and consumer protection thereunder.

The present chapter, undertakes the study of the widespread interplay of information and communication technologies (ICTs) with and their applications to global economic processes, including international trade and business enterprises. The chapter particularly examines the ICT indicators for development, including e-commerce, the ongoing trends and their impact. Moreover, this chapter undertakes an in-depth study in various aspects of International legal framework on e-commerce and e-commerce related aspects.

4.1 Introduction

Global economic processes, including international trade, are increasingly influenced by the creation, dissemination, accumulation, and application of information and knowledge. Development can no longer be understood without taking into consideration the widespread effects of information and communication technologies (ICTs) and their applications to enterprises.

From a development point of view, one must also investigate how and to what extent the enterprises of developing countries are adopting ICTs and e-commerce structures, and whether their patterns of adoption and use are (or should be) different from those of their counterparts in developed countries. It is then necessary to examine the internal divides in developing countries that limit the chances that groups such as the poor, rural communities and women will be able to benefit from ICTs in terms of better economic opportunities. The participation of developing countries in international trade in ICT goods and services is another fundamental aspect of their involvement in the global information economy. Lastly, one should try to quantify the impact of ICTs at the micro and macro levels, particularly with regard to their effects on growth and economic development.

4.1.1 ICT Indicators for Development: Trends and Impact

In 2018, the Internet and its applications continued to penetrate societies and economies around the globe. Mobile communications continued their steep growth in developing countries, which are now far ahead of developed countries in terms of an absolute number of subscribers. Mobile phones also continue to be the only ICT indicator where developing countries have surpassed developed countries. Despite this growth, internet penetration rates in many developing countries remain low, especially among the least developed countries (LDCs). The Internet users' curve continues to flatten in most developed countries; at the same time, broadband is experiencing unprecedented growth in rich countries, providing them with unexpected opportunities for economic growth and job creation.[1] This flies in the face of reality in many developing countries, where most of the small and medium sized enterprises (SMEs)[2] depend on slow, low-quality connections unsuitable for most e-business applications.

This section will provide an overview of trends and indicators on the use of ICTs by different factors in society and the economy, as well as its impact on development, growth, and trade.

[1] Information Economy Report, 2019

[2] Small and medium-sized enterprises (***SMEs***) or small and medium-sized businesses (SMBs) are businesses whose personnel numbers fall below certain limits. The abbreviation "***SME***" is used by international organizations such as the World Bank, the European Union, the United Nations and the World Trade Organization (WTO).

4.1.2 ICT Indicators in E-commerce Through the Use of Mobile Phones

Mobile phones are the only ICT indicator in which developing countries have surpassed developed countries in terms of users (see figure 4). Furthermore, mobile phones have economic importance for many users in developing countries, as they are enablers of business at large and particularly, for micro-entrepreneurs. The economic benefits of mobile phone usage is a relevant factor for the growth in the number of mobile phone subscribers in developing countries. The evolution and the growing share of developing economies in the worldwide mobile market can be seen in figure no.1 given herein below:

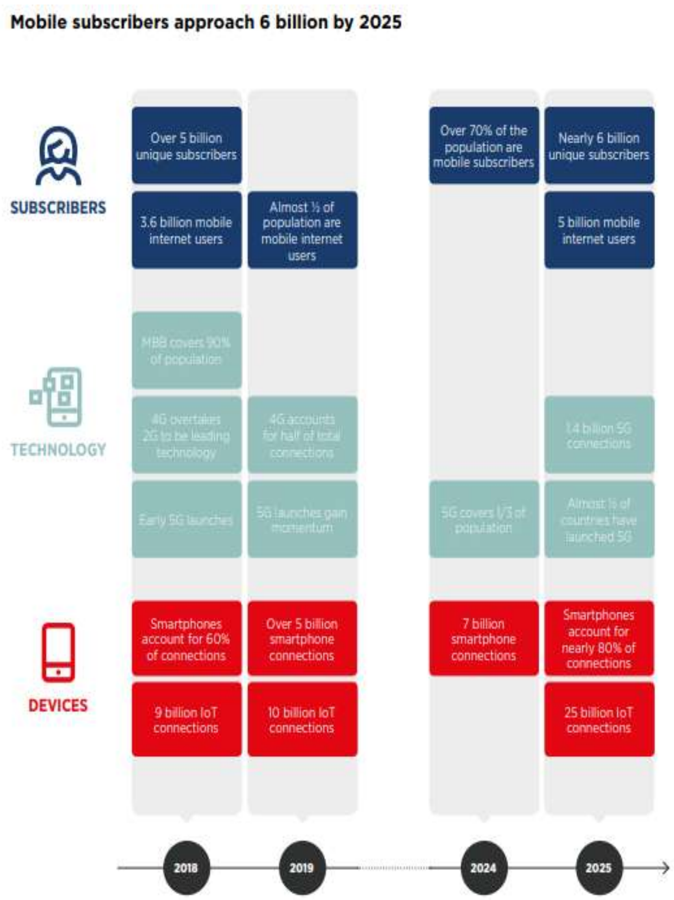


Figure No. 1 Mobile phone subscribers by the level of development Source: GSMA Intelligence Report 2019

Mobile phones are particularly playing a vital role in e-commerce. In 2018, mobile technologies and services generated 4.6% of GDP globally, a contribution that amounted to $3.9 trillion of economic value-added. The mobile ecosystem also supported almost 32 million jobs (directly and indirectly) and made a substantial contribution to the funding of the public sector, with more than $500 billion raised through general taxation. By 2023, mobile's contribution will reach $4.8 trillion (4.8% of GDP) as countries around the globe increasingly benefit from the improvements in productivity and efficiency brought about by increased take-up of mobile services. Furthermore, 5G technologies are also taking root across the globe. 5G signifies the fifth generation of cellular networks and is the fastest form of internet network at present. It is expected that 5G technologies are to contribute $2.2 trillion towards the global economy over the next 15 years, with key sectors such as manufacturing, utilities and professional/financial services benefiting the most from the new technology.[3]

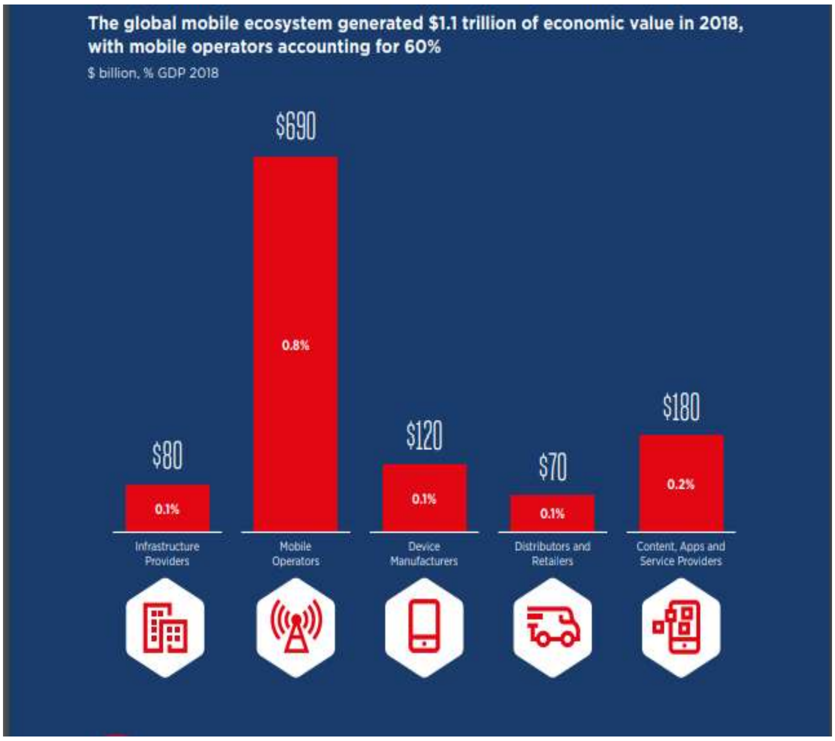


Figure No. 2 shows global mobile economy

Source: GSMA Intelligence Report 2019

[3]The Mobile Economy 2019, *available* at https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=39256194&file=2712-250219-ME-Global.pdf (last visited on February 16, 2019)

In 2018, the mobile ecosystem contributed more than $500 billion to the funding of the public sector through general taxation.

5G is set to power billions of connections and be the network infrastructure for the Internet of everything. It promises to reinvent the business world, solve problems we haven't yet encountered and have a major impact on every aspect of our digital lives.[4]

5G will raise the portable system to interconnect individuals, yet in addition, interconnect and control machines, articles, and gadgets. It will convey new degrees of execution and proficiency that will enable new client encounters and interface new businesses. 5G will convey multi-Gbps pinnacle rates, ultra-low inactivity, enormous limit, and progressively uniform client experience.

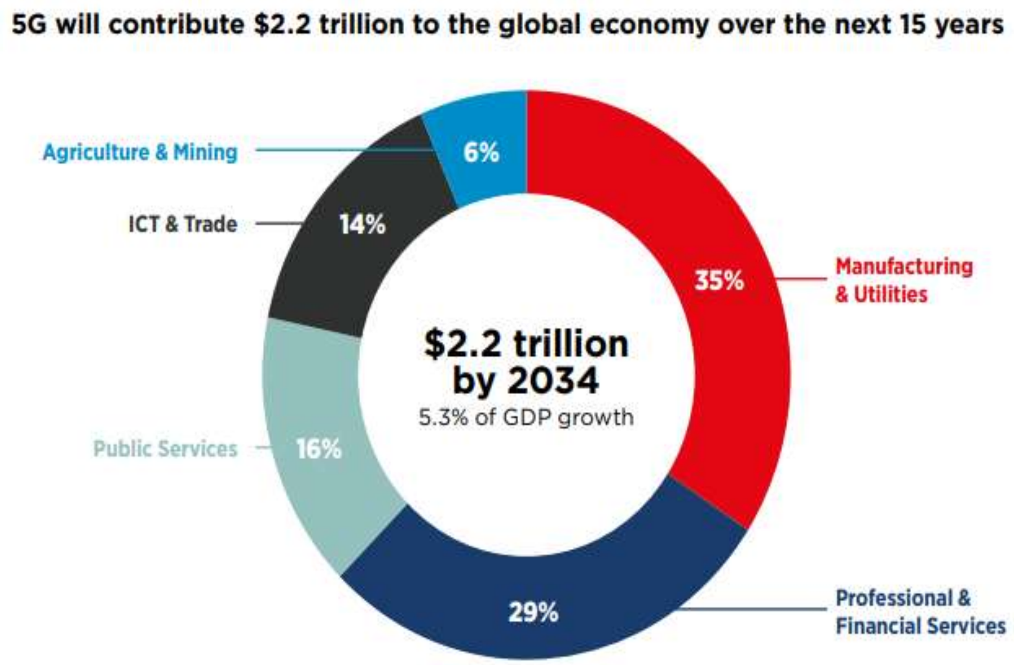


Figure No. 35G technology's global economy

Source: GSMA Intelligence Report 2019

[4] The trillion dollar race: what 5G means to the global economy, *available* at https://www.orange-business.com/en/blogs/trillion-dollar-race-what-5g-means-global-economy,(last visited on February 16,2019)

a) Mobile Phones Delivering Social Impact:

As the availability gap closes, versatile web selection will progressively turn into the key measurement by which to measure and assess the worth of mobile phones by the portable business, including its commitment to the UN’s Sustainable Development Goals (SDGs). Three years into the 2030 Agenda for Sustainable Development, mobile commerce is expanding its effect over every single one of the 17 SDGs because on account of the extensively versatile reach and efficient use. Furthermore, there is an added benefit to developing countries on account of the portable use of such devices since they effectively spike the digitization of frameworks, procedures, and partner communications over various ventures, including agribusiness, infrastructure, health sector, education sector, social insurance, etc.

b) Deployment of Infrastructure and Networks:

The mobile industry drives impact through the provision of and investment in high-performing mobile networks, which provide the foundations for the digital economy and act as a catalyst for a diverse and innovative range of services. By the end of 2018, 3G coverage reached more than 90% of the world’s population, while over 80% of the global population were covered by a 4G network.

According to InMobi's Annual Guide to Mobile Marketing 2021, in the COVID-19 pandemic, India has become the first mobile user economy in 2020. According to a report, the consumer market industry on mobile, India will account for about 14% of global app installations by 2020. India ranks second in average time spent on mobile devices, up 37% in the first half of 2020.[5]

c) Access and Connectivity:

Mobile operators are continuously striving to connect the unconnected and these efforts have fructified in achieving more than half a billion new

[5] India transformed itself into a mobile-first consumer economy in 2020, *Available* at https://www.thehindubusinessline.com/info-tech/india-transformed-itself-into-a-mobile-first-consumer-economy-in-2020-report/article33609247.ece *(last visited on June 20, 2021)*

mobile subscribers since 2015. An increasing number of people are moving beyond voice calls to adopt mobile internet services, enabling them to participate in the digital economy. Since 2015, there have been over 850 million new mobile internet users, bringing the total to 3.6 billion people globally.

d) Enabling Services and Relevant Content:

Mobile technology has enabled a range of life-enhancing services such as mobile financial services, mobile agriculture, and mobile health. By the end of 2018, there were 866 million registered mobile money accounts worldwide, helping to expand financial and social inclusion. Meanwhile, emerging areas such as the Internet of Things (IoT)[6], big data and artificial intelligence are demonstrating their potential for transformative impacts on lives.

In 2019, the number of mobile phone subscribers worldwide was at 5.112 billion, and the total population of the world is 7.776 billion.[7] In developed countries, the growth in the mobile phone industry has come from increased offer and use of innovative services, from SMS, free calling facilities, cheap internet, roaming facility, effective and easy Internet access and additional entertainment features like music downloads, movie streaming, social media, etc.

[6] The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.
[7]Digital 2019 global internet use accelerates, *available* at https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates (last visited on Feburary16,2019)

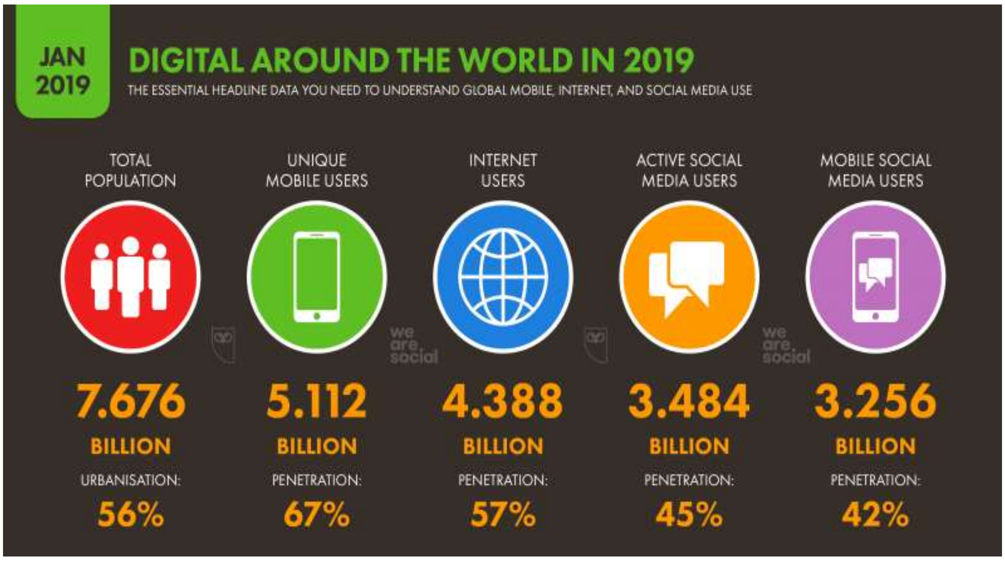


Figure No. 4

Source (Digital Economy Report 2019, Hootsuite and We Are Social)

Mobile connectivity sidesteps some important obstacles to other types of connectivity, but most notably to the deployment of the fixed-line mega structure, which can be hampered by, among other things, cost and the remoteness of certain areas. In Africa, mobile phones have proved so successful that in many cases they have replaced fixed lines.

The digital economy report, 2019 shows the key patterns, experiences and indicates the basic features of the digital revolution underway in order to improve our understanding.[8] These features are as follows:

- There were 5.11 billion mobile subscribers on the global scenario as in 2019 and this indicates an increase of 100 million (2 percent) in the previous year.
- There were 4.39 billion web users in 2019, an expansion of 366 million (9 percent) versus January 2018.
- There were 3.48 billion internet users active on social media in 2019, with around 288 million (9 percent) increase in such social media users since the

[8] *Id*. at 6

previous year. Furthermore, out of which, 3.26 billion individuals were active on social media through their mobile phones as of January 2019. This accounted for a significant increase by 297 million new users accounting for a 10 percent increase on a year by year increment.

e) Internet

Internet is the network in its entirety, made up of thousands of individual networks, all of which can interact with each other and are interconnected. E-commerce, as we understand it today, has become a possibility today on account of the internet and World Wide Web.

Between 2018 and 2019, the number of Internet users worldwide, as well as Internet penetration, continued to grow significantly, as shown in figure 2 and 3 show the number of Internet users and Internet.

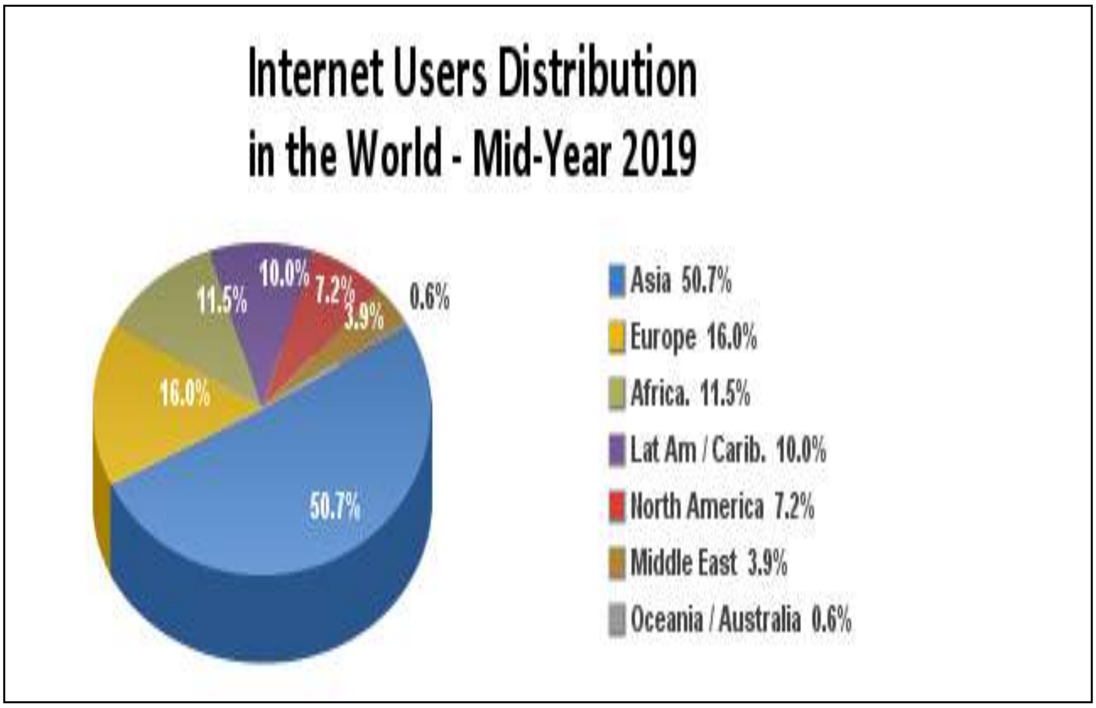


Figure No. 5

Source: Internet World Stats[9]

[9] Internet World Stats, *available* at www.internetworldstats.com (last visited on March 24,2019)

In 2019, Asia accounted for nearly 50% of all Internet users, almost a third of whom were in India and China while internet users in Europe and America accounted for only 33.2%.

Internet usage in the country has exceeded half a billion people for the first time, pegged at 566 million, significantly driven by rural internet growth and usage. Furthermore, India's internet users were expected to register double-digit growth to reach 627 million in 2019, primarily driven by rapid internet growth in rural area.[10]

WORLD INTERNET USAGE AND POPULATION STATISTICS 2019 Mid-Year Estimates						
World Regions	Population (2019 Est.)	Population % of World	Internet Users 30 June 2019	Penetration Rate (% Pop.)	Growth 2000-2019	Internet World %
Africa	1,320,038,716	17.1 %	522,809,480	39.6 %	11,481 %	11.5 %
Asia	4,241,972,790	55.0 %	2,300,469,859	54.2 %	1,913 %	50.7 %
Europe	829,173,007	10.7 %	727,559,682	87.7 %	592 %	16.0 %
Latin America / Caribbean	658,345,826	8.5 %	453,702,292	68.9 %	2,411 %	10.0 %
Middle East	258,356,867	3.3 %	175,502,589	67.9 %	5,243 %	3.9 %
North America	366,496,802	4.7 %	327,568,628	89.4 %	203 %	7.2 %
Oceania / Australia	41,839,201	0.5 %	28,636,278	68.4 %	276 %	0.6 %
WORLD TOTAL	7,716,223,209	100.0 %	4,536,248,808	58.8 %	1,157 %	100.0 %

Figure No. 6 Internet User, 2019

Source: Internet World Stats

Internet access by enterprises in the developing world is less uniform, reflecting a very broad range of Internet penetration rates. This suggests that

[10] Internet users in India, *available* at https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-to-reach-627-million-in-2019-report/articleshow/68288868.cms (last visited on March 24,2019)

the level of ICT knowledge in the economy might also be an important determinant of Internet use by enterprises since setting up a website demands more than basic computer literacy. Furthermore, it could be indicative of the fact that the characteristics of a country's economy and the structure of the enterprise sector may cause differing predispositions for Internet use. Enterprises involved in more knowledge-intensive production tend to demand greater Internet access and so do large enterprises as compared to smaller firms.

4.2 Tool and Technique of E-commerce in 2021

4.2.1 Artificial Intelligence (AI)

Artificial intelligence is based on the principle that human intelligence can be defined in a way that a machine can easily mimic it and execute tasks, from the most simple to those that are even more complex. The goals of artificial intelligence include learning, reasoning, and perception.[11]

Artificial intelligence also has applications in the financial industry, where it is used to detect and flag activity in banking and finance such as unusual debit card usage and large account deposits all of which immensely help the bank's fraud department. AI is also being used to help streamline and make trading easier. This is done by making supply, demand, and pricing of securities easier to estimate.[12]

4.2.2 Smart Home Devices

In the recent years have seen a fast increment in the utilization of home digital innovation in the U.S. The advanced transformation (particularly in the realm of IoT) has powered an energizing new stage with organizations in the home mechanization industry, offering buyers better than ever-brilliant home innovations and offering ascend to a completely

[11] Artificial intelligence, *available* at: www.investopedia.com/terms/a/artificial-intelligence-ai.asp (last visited on February 17,2019)
[12] *Ibid*

interconnected, simple to-control condition named the "savvy home". These gadgets offer customers remote control checking of basic family gadgets and improved utility investment funds. Some smart home technologies are as follow:

a) Alexa

Amazon Alexa, known simply as Alexa, is a virtual assistant AI[13] developed by Amazon, first used in the Amazon Echo and the Amazon Echo Dot smart speakers developed by Amazon Lab126. It is capable of voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, playing audiobooks, and providing weather, traffic, sports, and other real-time information, such as news. Alexa can also control several smart devices using itself as a home automation system.

Alexa for Business is a paid subscription service allowing companies to use Alexa to join conference calls, schedule meeting rooms and get custom skills designed by 3rd party vendors. At the launch of the device, notable skills such as, notable skills are available from SAP, Microsoft, and Salesforce. As of November 2018, Amazon had more than 10,000 employees working on Alexa and related products. In January 2019, Amazon's devices team announced that it had sold over 100 million Alexa-enabled devices.[14]

b) Google assistant

Google Assistant is an artificial intelligence-powered virtual assistant created by Google that is essentially accessible on portable and home gadgets. In contrast to the organization's previous virtual assistant, Google Now, the Google Assistant can take part in two-manner discussions.

Google Assistant offers voice commands, voice searching, and voice-activated device control, letting you complete a number of tasks after you've

---

[13] Virtual assistant AI , *available* at: www.wikipedia.com (last visited on May 02,2019)
[14]Amazon Alexa, *available at* https://en.wikipedia.org (last visited on May 02,2019)

said the “OK Google” or “Hey, Google” wake words. It is designed to give you conversational interactions.[15]

Google Assistant will:

- Control your devices and your smart home
- Access information from your calendars and other personal information
- Find information online, from restaurant bookings to directions, weather and news
- Control your music
- Play content on your Chromecast or other compatible devices
- Run timers and reminders
- Make appointments and send messages
- Open apps on your phone
- Read your notifications to you
- Real-time spoken translations

c) Siri

Siri is a virtual assistant that is part of Apple Inc.’s iOS, iPadOS, watchOS, macOS, and tvOS operating systems. The assistant uses voice queries and a natural-language user interface to answer questions, make recommendations, and perform actions by delegating requests to a set of Internet services. The software adapts to users’ individual language usages, searches, and preferences, with continuing use. Returned results are individualised.[16]

---

[15]What is google assistant how does it work and which devices offer it *available at* https://www.pocket-lint.com/apps/news/google/137722-what-is-google-assistant-how-does-it-work-and-which- devices-offer-it (last visited on April 28,2019)

[16] Siri, *available at* https://en.wikipedia.org/Siri (last visited May 2,2020)

d) Web entertainment channel

A web arrangement is a progression of scripted or non-scripted recordings, for the most part in verbose structure, released on the Internet and part of the web TV medium, which initially arose in the late 1990s and turned out to be progressively conspicuous in the mid-2000s. A solitary example of a web arrangement program can be called a scene or "webisode", however, the last term isn't frequently utilized. All in all, web arrangement can be viewed across a range of stages and gadgets, including work area, workstation, tablets, and cell phones.

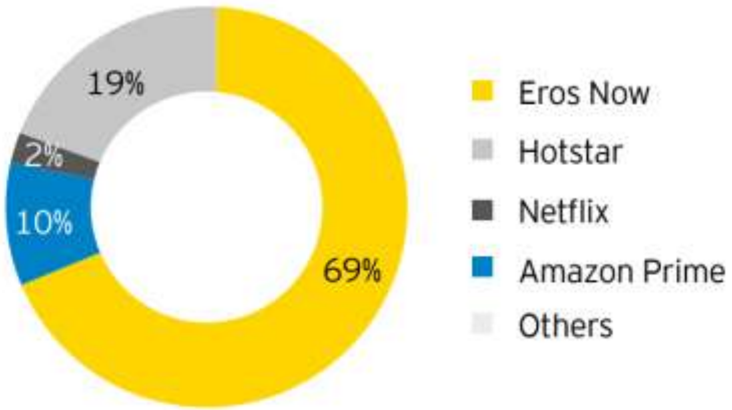


Figure no.7

Source https://www.moneycontrol.com

In terms of television shows, Hotstar and Netflix are ahead of the curve, but Eros Now has the lion's share of original movies streaming on its platform. Eros Now holds the rights to 69 percent of all movies available for streaming in 2017, as opposed to 19 percent for Hotstar and 10 percent for Amazon Prime.

The streaming ecosystem in the country might still be in a nascent state, but India has the second-largest online video audience, more than Brazil and the United States. Ernst & Young estimates that India had 250 million video consumers in 2017, 190 million of those who were between the ages of 15 and 34. An increase in internet speed, a fall in data tariffs and greater internet penetration could double the number of digital video consumers to 500 million by 2020.[17]

e) Social media

Social media commerce is an amazing route for any business of all sizes in order to reach out to the possible and existing customers. Consumers are nowadays continuously accessing social media and finding new brands and communicating with previously used brands through social media. A company not using social media like Facebook, Twitter, Instagram and Pinterest, may be passing up a major opportunity for getting some extraordinary advertising. Social media has driven up customer base and sales for innumerable businesses, helped carry them to achieve some striking accomplishments and publicising and driving offers and deals.

One of the characterizing marvels of the present occasions reshaping the world as we probably are aware of it, is the overall openness to the web. The lovechild of the World Wide Web is digital life, which comes in numerous structures, including web journals, gatherings, business systems, photograph sharing stages, social gaming, microblogs, talk applications, and to wrap things up interpersonal organizations. Brands are riding the rush of web-based life promoting themselves. This is significantly reflected from the fact that 73% of advertisers accept that their endeavours through online social media promotion has been “to some degree compelling” or “exceptionally viable” for their business.

[17]The rise of ott players streaming platforms and the threat to the box office, *available* at https://www.moneycontrol.com/news/trends/entertainment/the-rise-of-ott-players-streaming-platforms-and-the-threat-to-the-box-office-2688531.html (last visited on April 25,2019)

Figure No. 8

Source Influencer Marketing Hub, February 15th, 2020

Figure shows that in every 8 minutes 16 second active users on YouTube are 38,745,040, on twitter are 4,182,272 and on Instagram are 449,376. Thus, social media plays a vital role in e-commerce industry. Furthermore, this is a new phenomena of marketing.

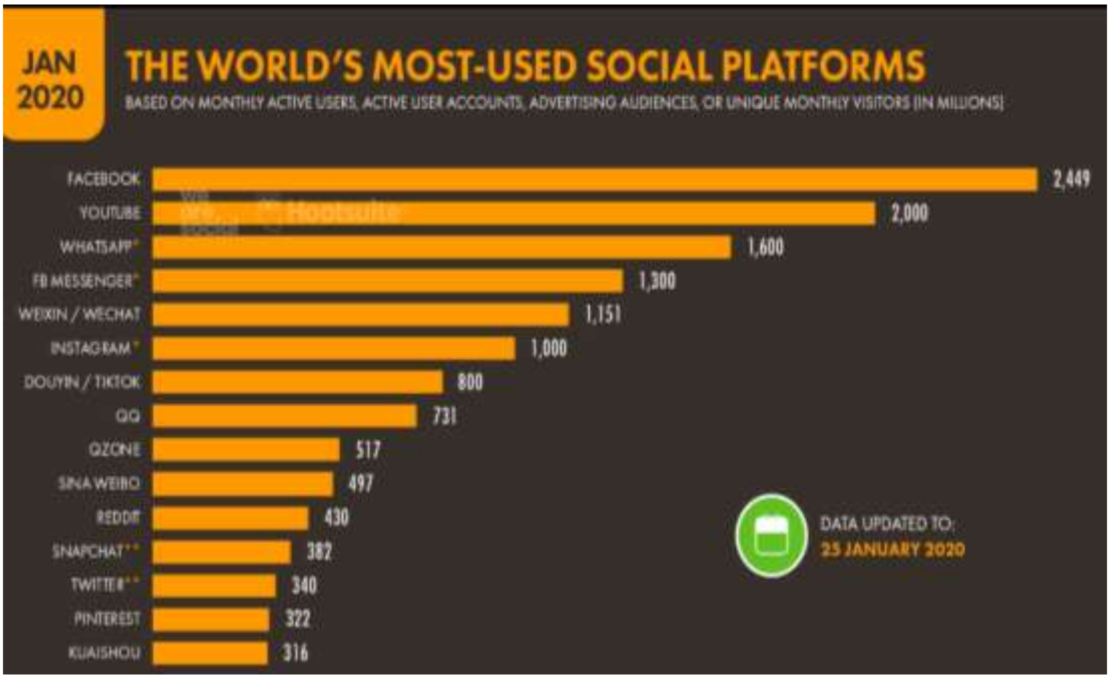


Figure No. 9

Source https://datareportal.com/social-media-users

Figure No. 9 shows that web-based social media presently has over 300 million or more month to month dynamic users:

- Facebook has 2.45 billion month to month dynamic clients.
- YouTube has 2 billion month to month dynamic clients.
- WhatsApp has 1.60 billion month to month dynamic clients.
- Facebook Messenger has 1.30 billion month to month dynamic clients.
- WeChat (Weixin) has 1.15 billion month to month dynamic clients.
- Instagram has 1 billion month to month dynamic clients.
- TikTok (Douyin) has 800 million month to month dynamic clients.
- QQ has 731 million month to month dynamic clients.
- QZone has 517 million month to month dynamic clients.
- Sina Weibo has 497 million month to month dynamic clients.
- Reddit has 430 million month to month dynamic clients.
- Snapchat’s latent capacity publicizing reach is around 382 million dynamic clients.

With economic structures involving local and regional entities, expanding into global and transnational entities, it is undeniable that technology has played a vital role in making this possible. All major world economies are striving to enhance their international presence and as discussed above, the various tools and techniques relating to e-commerce have been highly facilitative. However, the exponential growth of the e-commerce sector has raised grave concern with regards to the regulation and proper resolution of issues pertaining to this mode of commerce which transcends the traditional jurisdiction of existing laws and often involves transactions involving persons belonging to two or more countries. It is therefore pertinent to analyse at this stage the development of the new dimensions of law which provide critical international legal framework on e-commerce at a multinational/global level.

4.3 International Legal Framework on E-Commerce

Increasingly, traditional laws are being adapted and applied to new legal issues stemming from the use of this new medium, the Internet, to conduct business transactions. Additionally, new laws are being created to deal specifically with such issues. Frequently, people use the term cyber law to designate the emerging body of laws (consisting of court decisions, newly enacted or amended statutes, and so on) that governs cyberspace transactions. Cyber law is not really a classification of law, rather, it is an informal term used to describe how traditional classifications of law such as civil law and criminal law, similarly it is being applied to online activities.[18]

Anyone preparing to enter today's business world will find it useful to know how old and new laws are being applied to activities conducted online, such as advertising, contracting, and banking, filing documents with the courts or government agencies, employment relations and a variety of other transactions. For that reason, this text is devoted entirely to this topic. Special features throughout the text also focus on how technology, and particularly the use of the Internet, is transforming the business world.[19]

As it is known to everybody that cutting edge global law is a piece of European legitimate framework and over and over it has been developed in an extensive way. Presently global law is a different and unmistakable unit in the English legal framework, the same amount as in the law of insolvency or of agreements, yet it has this solidarity, not on the grounds that it manages one specific subject, but since it is constantly relevant in terms of at least one of these three inquiries, which are:

[18] Miller Roger Leroy and Jentz Gaylord A., *Law for E-Commerc*e, 16,(west Thomson learning, 2002)
[19] *Ibid*

- Jurisdiction of the Courts
- The choice of law
- Jurisdiction

Today everybody is mindful about the way that on account of the digital revolution the world seems to have become smaller. As of now, the preceding chapters have examined the e-commerce model and referred to its importance. However, the reason why international laws are pertinent in this regard can be understood from the fact that due to the digitisation of commerce, today a person sitting in India can enter into a contract with someone situated in another country. Thus International legislations are relevant since it reflects upon the initiative of the UN in developing and putting in place a legal framework of model laws to regularise e-contracts. Following are the some examples of such legal frameworks pertaining to e-contracts and e-commerce:

- UNCITRAL Model Law on Electronic Commerce
- United Nations Convention on Contracts for the International Sale
- UNCITRAL Model Law on Electronic Signatures
- The United Federal Trade Commission Can-Spam Act, 2003
- European Union Directive, 2000
- Anti-cybersquatting Consumer Protection Act, 1999
- The Hague Conference on Private International Law, 1995 and 1999
- WTO rules on e-commerce
- The Organisation for Economic Co-operation and Development (OECD)
- Singapore, the Electronic Transactions Act, 1998
- United Nations Guidelines for Consumer Protection (UNGCP)

4.4. UNCITRAL Model Law on E-commerce

The MLEC was the first legislative text to adopt the fundamental principles of non-discrimination, technological neutrality and functional equivalence that are widely regarded as the founding elements of modern electronic commerce law. The principle of non-discrimination ensures that a document would not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form. The principle of technological neutrality mandates the adoption of provisions that are neutral with respect to technology used. In light of the rapid technological advances, neutral rules aim at accommodating any future development without further legislative work. The functional equivalence principle lays out criteria under which electronic communications may be considered equivalent to paper-based communications. In particular, it sets out the specific requirements that electronic communications need to meet in order to fulfil the same purposes and functions that certain notions in the traditional paper-based system seek to achieve, for example, “writing” “original”, “signed”, and “record”.[20]

The international standard for removing statutory barriers to electronic commerce is the United Nations Commission on International Trade Law (UNCITRAL) on e-commerce, was recommended with a mandate to progressive harmonization and unification of the law of international trade in 1996 and in that respect to bear in mind the interests of all peoples, in particular those of developing countries, in the extensive development of international trade.[21]

For the execution of the objectives of UNCITRAL[22] and at the same time number of transactions in international trade were carried out by means of electronic data interchange and other means of communication, commonly referred to as electronic commerce, so it felt to adopt MLEC. The main feature of model law is minimalistic, which is to say that it does not prescribe in detail how to create legally bound electronic documents. It does not require the use of any particular technology to meet legal requirements and model law provides functional equivalence by which electronic documents are legally effective if

[20] Uncitral model law on e-commerce *available at* https://uncitral.un.org (last visited on May 16, 2020)
[21] Alwyn Didar Singh *E-Commecrce in India : Assessments and Strategies for the Developing World*,63(LexixNexix ButterWorths india2008)
[22] *Ibid*

they satisfy the same policy functions as the paper documents as required by the law.[23]

The utilization of present-day methods for correspondence, for example, electronic mail and electronic information exchange (EDI) for the lead of worldwide exchanges has been fast expanding and is expected to grow further with the growth of specialized backing. For example, information highway and the Internet become all the more broadly open. However, the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such messages, or by uncertainty as to their legal effect or validity. The purpose of the Model Law is to offer national legislators a set of internationally acceptable rules as in order to assist them to avoid and remove legal obstacles and how to put in place a more secure legal environment for electronic commerce. The standards communicated in the Model Law are likewise expected to be useful also to singular clients of electronic trade in the drafting of a portion of the authoritative arrangements that may be expected to conquer the lawful hindrances to the expanded utilization of electronic commerce.

The choice of framing UNCITRAL as model legislation on electronic commerce was made in light of the way that in various nations the current enactment administering correspondence and capacity of data is insufficient or obsolete on the grounds that it doesn't think about the utilization of electronic commerce. In certain cases, existing legislation imposes or implies restrictions on the use of modern means of communication, for example by prescribing the use of written, signed or original documents. While a few countries have adopted specific provisions to deal with certain aspects of electronic commerce, there exists no legislation dealing with electronic commerce as a whole. This may bring about vulnerability with regards to the lawful nature and legitimacy of data presented in a structure other than a traditional paper

[23] Brinson j Dianne , Radcliffe F. mark, *Internet law and business handbook*,291 (Quality Books inc (2000)

document. Besides, while sound laws and practices are fundamental in all nations where the utilization of EDI and electronic mail is getting across the board, this need is additionally felt in numerous nations concerning such correspondence systems as telecopy and telex messaging. The Model Law may also help to remedy disadvantages that stem from the fact that inadequate legislation at the national level creates obstacles to international trade, a significant amount of which is linked to the use of modern communication techniques. Disparities among, and uncertainty about, national legal regimes governing the use of such communication techniques may contribute to limiting the extent to which businesses may access international markets.[24]

Moreover, at a universal level, the Model Law might be helpful in specific cases as an instrument for deciphering existing international conventions, treaties and other international instruments that create legal obstacles to the use of electronic commerce, for example by prescribing that certain documents or contractual clauses be made in written form. As between those State parties to such international instruments, the adoption of the Model Law as a rule of interpretation might provide the means to recognize the use of electronic commerce and obviate the need to negotiate a protocol to the international instrument involved.

The goals of the Model Law, which incorporate empowering or encouraging the utilization of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed in the Model Law in its national legislation for those situations where gatherings select to utilize electronic methods for correspondence, it would bring efficiency, clarity and ease of doing electronic business.

[24] What is EDI, *available at* https://www.edibasics.com (last visited on July 20,2019)

4.4.1 Scope of Model Law

The title of the Model Law alludes to electronic commerce. While the meaning of electronic data interchange (EDI) is given in Article 2, the Model Law does not specify the meaning of electronic commerce per se. In preparing the Model Law, the Commission decided that, in addressing the subject matter before it, it would have in mind a broad notion of EDI, covering a variety of trade-related uses of EDI that might be broadly referred under the rubric of electronic commerce, although other descriptive terms could also be used. Among the means of communication encompassed in the notion of electronic commerce are the following modes of transmission based on the use of electronic techniques: communication by means of EDI defined narrowly as the computer-to-computer transmission of data in a standardized format; transmission of electronic messages involving the use of either publicly available standards or proprietary standards; transmission of free-formatted text by electronic means, for example through the internet. It was likewise noticed that, in specific conditions, the idea of electronic business may cover the utilization of procedures, for example, telecopy and telex.[25]

It ought to be noticed that, while the Model Law was drafted with steady reference to the more digital communication techniques, e.g., EDI and electronic mail, the principles on which the Model Law is based, as well as its provisions, are intended to apply also in the context of less advanced communication techniques, such as telecopy.[26] There may exist situations where digitalized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of telecopy of a computer print-out. A data message may be initiated as oral communication and end up in the

[25] https://www.uncitral.org/pdf/english/texts/arbitration/ml-arb/06-54671_Ebook.pdf (last visited on April 25,2019)
[26] *Id.* at 20

form of telecopy, or it may start as telecopy and end up as an EDI message. A characteristic of electronic commerce is that it covers programmable messages, the computer programming of which is the essential difference between such messages and traditional paper-based documents. Such situations are intended to be covered by the Model Law, based on a consideration of the users need for a consistent set of rules to govern a variety of communication techniques that might be used interchangeably. More generally, it may be noted that, as a matter of principle, no communication technique is barred from the scope of the Model Law since future technical developments need to be accommodated.

The destinations of the Model Law are best served by the broadest conceivable utilization of the Model Law. Thus, although there is provision made in the Model Law for the exclusion of certain situations from the scope of Articles 6, 7, 8, 11, 12, 15 and 17, an enacting State may well decide not to enact in its legislation substantial limitations on the extent of utilization of the Model Law.[27]

The Model Law should be viewed as a balanced and discrete set of rules, which are recommended to be enacted as a single statute. Contingent upon the circumstance in each authorizing State, in any case, the Model Law could be executed in different manners regardless; the Model Law could be completed in various habits, either as a solitary rule or broken into a number of pieces of enactment.

4.4.2. Structure of MLEC

The Model Law is divided into two parts, one dealing with electronic Commerce in general and the other one dealing with electronic commerce in specific areas. In that context, the model law bars any discrimination against electronic documents or data message on the sole

[27] Uncitral model law on international commercial arbitration, *available at* https://www.trans-lex.org/450900/_/uncitral-model-law-on-international-commercial-arbitration/ (last visited on April 25,2019)

ground that they are in electronic form. The model law states that shreds of evidence shall not be inadmissible only because of its electronic form, under certain situations, and that people can retain electronic records to satisfy record retention laws.

The issue is the possible electronic legislation. This issue is of principal importance, and decisions as to the application of possible legislation will require careful consideration of possible exceptions to coverage.

4.4.3. Definitions

It is clear that the language of electronic commerce is still developing. A number of definitions, including specifically technical ones, are being developed, but it is not always the case that these are appropriate for inclusion in a legal text. International texts, such as the International Chamber of Commerce's General Usage for International Digitally Ensured Commerce (GUIDEC)[28] is being developed. This text intends to serve as an indicator of the terms involved in electronic commerce and to provide a general background to the issues raised by these terms. It also aims to set out standard practices or recommendations relating to ensuring or securing authentication of digital information. To an extent, these international texts represent both civil and common law treatment of the subject matter, it present both businesses and governments with a comprehensive statement of best practices for the emerging global infrastructure.[29]

The Model law explains some electronic terminology which need uniformity and consistency among jurisdictions. Such as Data message,

[28] (This General Usage for International Digitally Ensured Commerce (GUIDEC) has been drafted by the International Chamber of Commerce (ICC) Information Security Working Party, under the auspices of the ICC Electronic Commerce Project. The ICC Electronic Commerce Project is an international, multidisciplinary effort to study, facilitate and promote the emerging global electronic trading system. Existing ICC Commissions participating in the Electronic Commerce Project include the commissions on Banking, Air Transport, Maritime and Surface Transport, Computing, Telecommunications and Information Policies, Commercial Practices, Financial Services and Insurance to provide a globally comprehensive approach to implementing digital commerce.GUIDEC

[29] Joga Rao, *Computer Contracts and Information Technology Law*, 2008 (2nd Ed., Vol.2, Wadhwa & Co., Nagpur, 2005)

Electronic Data Interchange (EDI), Originator, Addressee, Intermediary and Information system. The explanation of EDI and Data Message needs special discussion.

a) Electronic Data Interchange

The Model Law does not settle the question whether the definition of EDI necessarily implies that EDI messages are communicated electronically from computer to computer, or whether that definition, while primarily covering situations where data messages are communicated through a telecommunications system, would also cover exceptional or incidental types of situation where data structured in the form of an EDI message would be communicated by means that do not involve telecommunications systems. For example, the case where magnetic disks containing EDI messages would be delivered to the addressee by courier. However, irrespective of whether digital data transferred manually is covered by the definition of EDI, it should be regarded as covered by the definition of data message under the Model Law.[30]

EDI is the concept of businesses electronically communicating information that was traditionally communicated on paper, such as purchase orders and invoices. Technical standards for EDI exist to facilitate parties transacting such instruments without having to make special arrangements.[31]

Article 2 (b)[32] of the model law defines electronic data interchange and states that it includes sharing information between computer to computer by any electronic means is electronic data interchange, and digitally shared information by electronic resources is called electronic data interchange.

---

[30] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, *Available at* http://www.uncitral.org/pdf/english/texts/electcom/05-89450 _Ebook.pdf

[31]Electronic data interchange ,*available at* https://en.wikipedia.org (last visited on Feburay 19 ,2020)

[32] Model law on e commerce: “Electronic data interchange (EDI)” means the electronic transfer from computer to computer of information using an agreed standard to structure the information; s. 2 (b)

b) Data Message

The notion of data message is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication. Thus, the notion of the message includes the notion of a record. However, a definition of a record in line with the characteristic elements of writing in Article 6 may be added in jurisdictions where that would appear to be necessary.

The reference to similar means is intended to reflect the fact that the Model Law was not intended only for application in the context of existing communication techniques but also to accommodate foreseeable technical developments. The aim of the definition of a data message is to encompass all types of messages that are generated, stored or communicated in an essentially paperless form. For that purpose, all means of communication and storage of information that might be used to perform functions parallel to the functions performed by the means listed in the definition are intended to be covered by the reference to similar means, although, for example, electronic and optical means of communication might not be, strictly speaking, be similar. For the purposes of the Model Law, the word similar connotes functionally equivalent.

The definition of a data message is also intended to cover the case of revocation or amendment. A data message is presumed to have fixed information content but it may be revoked or amended by another data message.

Thus, it would be appropriate in the context of drafting legislation supporting electronic transactions to consider the adoption of purposes or interpretation provisions. While this issue is not considered further in this text, an interpretation or purpose provision could be based upon Article 3 of the Model Law. In this regard, reference to some of the national legislations may be referred which have put in place such purpose or interpretation provision such as the Uniform Electronic Transactions Act (US), the Illinois Electronic Commerce Security Act and Massachusetts Electronic Records and Signatures Act.

c) Legal Recognition of Data Messages[33]

Article 5 embodies the fundamental principle that data messages should not be discriminated against, i.e., that there should be no disparity of treatment between data messages and paper documents. It is intended to apply notwithstanding any statutory requirements for it to be in writing or an original. That fundamental principle is intended to find a general application and its scope should not be limited to evidence or other such matters. It should be noted, however, that such a principle is not intended to override any of the requirements contained in Articles 6 to 10. By stating that information shall not be denied legal effectiveness, validity or enforceability solely on the grounds that it is in the form of a data message, Article 5 merely indicates that the form in which certain information is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability. However, Article 5 should not be misinterpreted as establishing the legal validity of any given data message or of any information contained therein.

d) Evidence

A number of jurisdictions have legislative provisions dealing with the admissibility and evidential weight of electronic documents/data messages. These provisions, however, are not uniform, although a number of states are considering adopting uniform evidence laws.

e) Retention of Data Messages[34]

Article 10 establishes a set of alternative rules for existing requirements regarding the storage of information (e.g., for accounting or

[33] UN Model Law: Legal Recognition of data messages, art. 5
[34] UN Model Law : Retention of Data Messages, art. 10

tax purposes) that may constitute obstacles to the development of modern trade. Paragraph (1) of Article 10 is intended to set out the conditions under which the obligation to store data messages that might exist under the applicable law would be met. Following are the conditions:

i. the information contained therein is accessible so as to be usable for subsequent reference; and
ii. the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
iii. such information, if any, is retained which enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

Paragraph (2) of Article 10 covers a few elements transmittal information.

And Paragraph (3) provides that in meeting its obligations under paragraph (1), an addressee or originator may use the services of any third party, not just an intermediary.

4.4.4. Formation and Validity of Contracts[35]

Article 11 of the Model Law is not adopted to interfere with the law on the formation of contracts but rather to promote international trade by providing increased legal certainty as to the conclusion of contracts by electronic means. It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed.

Paragraph (1) covers not merely the cases in which both the offer and the acceptance is communicated by electronic means but also cases in which only the offer or only the acceptance is communicated electronically. As to the time and place of formation of contracts in cases where an offer or the

[35] UN Model Law: Formation and validity of contracts, art. 11

acceptance of an offer is expressed by means of a data message, no specific rule has been included in the Model Law in order not to interfere with national law applicable to contract formation.

4.4.5. Attribution of Data Messages[36]

Article 13 of the Model Law creates rules entitling the addressee to assume that a data message is that of the apparent originator (attribution) and that the data message as received is the same as that sent (message integrity). Article 13 moves beyond the existing common law position which applies to paper-based transactions by presumptively allocating the risk of loss arising from unauthorized or altered messages to the apparent originator rather that the addressee.

4.4.6. Time and Place of Dispatch and Receipt of Data Message[37]

Article 15 of the Model Law deals about time and place of dispatch and receipt of a data message. Paragraph (1) defines the time of dispatch of a data message as the time when the data message enters an information system outside the control of the originator, which may be the information system of an intermediary or an information system of the addressee. The concept of dispatch refers to the commencement of the electronic transmission of the data message. Where dispatch already has an established meaning, Article 15 is intended to supplement national rules on dispatch and not to displace them. If dispatch occurs when the data message reaches an information system of the addressee, dispatch under paragraph (1) and receipt under paragraph (2) are simultaneous, except where the data message is sent to an information system of the addressee that is not the information system designated by the addressee under paragraph (2)(a).

[36] UN Model Law: Attribution of data messages, art. 13
[37] UN Model Law: Time and place of dispatch and receipt of data messages, art. 15

The purpose of Paragraph (2) is to define the time of receipt of a data message and addresses the situation where the addressee unilaterally designates a specific information system for the receipt of a message (in which case the designated system may or may not be an information system of the addressee), and the data message reaches an information system of the addressee that is not the designated system. In such a situation, the receipt is deemed to occur when the data message is retrieved by the addressee. By designated information system, the Model Law is intended to cover a system that has been specifically designated by a party, for instance in the case where an offer expressly specifies the address to which acceptance should be sent. The mere indication of an electronic mail or telecopy address on a letterhead or other document should not be regarded as an express designation of one or more information systems.

Paragraph (3) is non-obstante in nature which states that Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

Paragraph (4) of Article 15 establishes an irrebuttable presumption regarding a legal fact, to be used where another body of law (e.g., on the formation of contracts or conflict of laws) requires determination of the place of receipt of a data message.

4.4.7. Carriage of Goods

Articles 16 and 17 contain provisions that apply equally to non-negotiable transport documents and to transfer of rights in goods by way of transferable bills of lading. The principles embodied in Articles 16 and 17 are applicable not only to maritime transport but also to the transport of goods by other means, such as road, railroad, and air transport.

Model Law[38] applies to any kind of information in the form of a data message used in the context[39] of commercial[40] activities. Model law provides for electronic contracts and regulates the attribution of the data message and the time and place of their sending and receipt, as well as the form of acknowledgment of receipt.

4.5. UNCITRAL Model Law on Electronic Signatures

The expanded utilization of electronic confirmation strategies alternative for written by hand marks and other conventional validation techniques has recommended the requirement for a particular legal structure to reduce uncertainty as to the legal effect that may result from the use of such modern techniques which may be referred to generally as electronic signatures. The risk that diverging legislative approaches be taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where lawful amicability just as technical interoperability is an attractive goal.

Building on the fundamental principles underlying Article 7 of the UNCITRAL Model Law on Electronic Commerce with respect to the fulfilment of the signature function in an electronic environment, this new Model Law is designed to assist States in establishing a modern, harmonized and fair legislative framework to address more effectively the issues of electronic signatures. In a modest but significant addition to the UNCITRAL Model Law on Electronic Commerce, the new Model Law offers practical standards against which the technical reliability of electronic signatures may be

[38] "This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."
[39] This Law does not override any rule of law intended for the protection of consumers
[40] The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

measured. In addition, the Model Law provides a linkage between such technical reliability and the legal effectiveness that may be expected from a given electronic signature. The Model Law adds substantially to the UNCITRAL Model Law on Electronic Commerce by adopting an approach under which the legal effectiveness of a given electronic signature technique may be predetermined (or assessed prior to being actually used). The Model Law is accordingly planned to cultivate the comprehension of electronic signature and the certainty with regards to certain electronic signature strategies that can be relied upon in determining the legality of critical transactions. Moreover, by establishing appropriate flexibility a set of basic rules of conduct for various parties that may become involved in the use of electronic signatures (i.e. signatories, relating to parties and third-party certification service providers) the Model Law may assist in shaping more harmonious commercial practices in cyberspace.[41]

The goals of the Model Law, which incorporate empowering or encouraging the utilization of electronic signatures and giving equivalent treatment to user of paper-based documentation and users of computer-based information, are essential for fostering economy and efficiency in international trade. By incorporating the procedures prescribed in the Model Law (and also the provisions of the UNCITRAL Model Law on Electronic Commerce) in its national legislation for those situations where parties opt to use electronic means of communication, the enacting State would appropriately create a media-neutral environment. The media nonpartisan methodology likewise utilized in the UNCITRAL Model Law on Electronic Commerce is expected to provide on a basic level, inclusion of every verifiable circumstance where data is created, put away or imparted, independent of the medium on which such data might be fastened. The words a media neutral environment, as used in the UNCITRAL Model Law on Electronic Commerce, reflect the principle of non-discrimination between information

[41] Arbitration.model.law, *available* at https://www.jus.uio.no/lm/un.1985/7.html, (last visited November 6,2019)

supported by paper medium and information communicated or stored electronically. The new Model Law equally reflects the principle that no discrimination should be made among the various techniques that may be used to communicate or store information electronically, a principle that is often referred to as technology neutral.

Article 7 is based on the recognition of the functions of a signature in a paper-based environment. Article 7 of the UNCITRAL Model Law on Electronic Commerce peruses as follows:

1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

a) method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

b) that method is reliable and was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3) The provisions of this article do not apply to the following:[42]

The Model Law on Electronic Signature doesn't bargain in any detail with the issues of risk that may influence the different gatherings parties with the activity of electronic signature systems. Those issues are left to applicable law outside the Model Law. However, the Model Law sets out criteria against which to assess the conduct of those parties, that is, the signatory, the relying party and the certification service provider.

[42] *Id.* at 40

Given the pace of technological development, the Model Law gives criteria to the lawful acknowledgment of electronic signatures irrespective of the technology used for example, digital signatures relying on asymmetric cryptography; biometric devices enabling the identification of individuals by their physical characteristics, whether by hand or face geometry, fingerprint reading, voice recognition or retina scan, etc. symmetric cryptography, the use of PINs; the use of tokens as a way of authenticating data messages through a smart card or other device held by the signatory; digitized versions of handwritten signatures; signature dynamics and other methods, such as clicking an OK-box. The various techniques recorded could be utilized in a blend to diminish foundational hazard.

The Model Law establishes as a basic principle that the place of origin, in and of itself, should in no way be a factor determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being legally effective in an enacting State. Determination of whether or the extent to which, a certificate or an electronic signature is capable of being legally effective should not depend on the place where the certificate or the electronic signature was issued but on its technical reliability. That basic principle is elaborated upon in Article 12.

4.6. Uniform Electronic Commerce Act (UECA)

The uniform law conference in Canada adopted the Uniform Commerce Act[43] of September 30, 1999, and recommended it for adoption by the member jurisdiction of the conference and to all the provinces and territories of Canada and the federal government.

The UECA was developed by a working group assembled on the internet representing private and public sectors in Canada and a handful of foreign contributors, which reached over 150 participants by the middle of

[43] The uniform commerce Act, *available* at http:/www.law.ualberta.ca/alri/ulc/currunt/uecafa.htm (last visited November 6,2019)

1999. The Act was debated at the annual meetings of the uniform law conference in 1998 and again 1999.

The UECA can be considered as a minimalist response to the quest for certainty in terms of the legal status of electronic communication and digital records. It is minimalist for several reasons:

First, the current law statutes and common law and private law based on contracts is capable of resolving a good number of questions on its own. Electronic message, even on the internet, do not present radically new questions in this regard and in every field.

Second, the digital underlying electronic records are changing rapidly, so attempts to prescribe specifically how to create legally effective communications risk obsolescence even before they come into force.

Third, the nature of e-commerce is global and users in general do not take a seriously different approach in this regard.

4.6.1. Scope of UECA

The Canadian Uniform Act covers not only commercial transactions but applies to all other rules of law that are not specifically excluded from it. That makes the list of exclusion important. Most of the list is itself a matter of international consensus, in that several of the laws that purport to enact UN model laws have put in place similar exclusions. The model law contemplated that enacting countries would exclude some laws from its rule but did not specify any per se. In Canada, people have also excluded the power of attorney for personal care and for the financial affairs of an individual. The concern of these kinds of documents was that they are often created by unsophisticated people, often without legal or technical advice. It was thought there was much risk of undetectable fraud or loss of integrity of data unless more specific security measures were provided, more than a uniform and fairly generic statute could give.

The scope section provides that the uniform Act yields to any computer statute that expressly regulates permits or prohibits the use of electronic communication. The conference thought its inappropriate to override legislated standard, even if the standard is out of date or inadequate. The point of the Model law is to remove barriers and provide safeguards for electronic communication, not to reform the law where the barriers have already been addressed. However, the Act provides that using words like “in writing “or “signed” does not constitute a prohibition against using electronic communication, since otherwise this exclusion would undermine the Act allows the operation of the Act itself.[44]

One purpose of the Uniform Act is to permit the user of electronic documents uniformly with consensus, without individually having to amend all the statues that could interrupt their use in any way. In case an authority learns after enacting an Act that some unnoticed statutory provisions should not be subject to the general permission, the Act allows the addition by regulation.

4.7. European Union E-Commerce Directives

The Directive consists of 24 Articles and 65 recitals. Recitals 17-52 elucidate the meaning of the Articles and recitals 53-65 contain some further considerations. Recitals 1-16 elaborate upon what the Directive is (not) aimed at, and as such gives a good impression of the scope of the Directive. In the first place these opening recitals i.e. 1-16, express the high expectations the European Union had with respect to electronic commerce (recital 2). Therefore, free movement of information society services (cf. Article 56 TFEU[45]) has to

---

[44] *Available* at http://www.cch.ca/_resources/pdf/ecommerce_slides_url.pdf (last accessed on April 24, 2018)

[45] Treaty on the Functioning of the European Union (TFEU) Article 56 prohibits restrictions on freedom to provide services within the Union in respect of nationals of Member States who are established in a Member State other than that of the person for whom the services are intended. Article 56 states “Within the framework of the provisions set out below, restrictions on freedom to provide services within the Union shall be prohibited in respect of nationals of Member States who are established in a Member State other than that of the person for whom the services are intended. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may extend the provisions of the Chapter to nationals of a third country who provide services and who are established within the Union.”

be realised through a high level of community (legal) integration (recital 1, 3-6).

The main objective of the Directive is to create a legal framework to cover certain legal aspects of electronic commerce in the internal market (recital 7-8) and that criminal law as such is not harmonised, and to ensure that freedom of expression is not affected (recital 8-9). Furthermore, the Directive must ensure the protection of minors and human dignity, consumer protection and the protection of public health, without prejudice to the level of protection in other Directives (recital 10- 11). The Directive does not deal with fiscal aspects (recital 12-13), privacy (recital 14), confidentiality of communication (recital 15), and gambling activities, with the exception of promotional games to encourage sale of goods or services (recital 16).[46]

Article 14 of the E-commerce Directive (2000/31) contains a restrictive obligation for digital service providers.[47] Under this arrangement, digital service providers can profit by a risk exclusion provided they: 1) don't have real information with regards to such illegal behaviour or of such data and, as such respects the claims of harm, which they did not know about in terms of its realities or conditions from which the criminal behaviour or data is apparent; 2) after acquiring such information or mindfulness, they act speedily to expel or to incapacitate the access to such data.

The provider of a hosting service can obtain knowledge about the illegal character of hosted content in a number of ways. For example, the provider could find such content through his own activities or he could be notified about the situation by a third party. Notifications could stem either from public authorities, i.e. courts or from private entities. In the latter case, the provider of the hosting service is called upon directly by a private individual to remove or

---

[46] E-commerce Directive | Shaping Europe's digital futur**e,** *available* at https://digital-strategy.ec.europa.eu (last visited June 7,2021)

[47] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive), OJ L 178, 17.07.2000, .*available* at https://www.jipitec.eu (last visited November 6,2019)

block access to the content in question. The mechanism is commonly referred to as 'notice-and-take-down'. It is the provider's task to assess whether such a complaint is credible and make a decision about the infringing character of the content.[48]

The E-Commerce Directive laid the groundwork for notice-and-take-down but did not provide any additional guidelines with regard to its implementation. Instead, the Directive left the subject matter open to the discretion of the Member States.[49] Article 16 and recital 40 of the Directive encourage self-regulation in this field. Certain Member States have developed more detailed, formal notice-and-take-down procedures, but the majority of the Member States opted for a verbatim transposition of the Directive, hoping that self-regulation would emerge.[50] This however it proved to be inefficient since most of countries never introduced any self-regulatory measures.[51] The result is that there is still a lack of any firm safeguards for the content removal procedures in most of the EU countries.[52]

As a result, the E-Commerce Directive and most national implementing laws place hosting providers in a position to decide which content can remain online and which should be removed. They may be considered as private 'gatekeepers', who are able to regulate the behaviour (and speech) of their users.[53] By providing conditional liability exemptions for third parties' illegal

---

[48] The Power of Positive Thinking:, *available* at https://www.jipitec.eu/issues/jipitec-8-3-2017/4623 (last visited June 7, 2021)

[49] E-Commerce Directive and Recital 46 E-Commerce Directive, art. 14.3

[50] T. Verbiest and G. Spindler *et al (eds)*., "Study on the Liability of Internet Intermediaries, Markt/2006/09/E'', 14-16, (November 2007) . For a more recent analysis of the national approaches to the problem of content regulation on the Internet see country reports accompanying the study by the Swiss Institute of Comparative Law, Comparative Study on Filtering, blocking and take-down of illegal content on the Internet – comparative considerations, Report commissioned by the Council of Europe, 20 December 2015

[51] P. Van Eecke and M. Truyens, "Legal analysis of a Single Market for the Information Society, New rules for a new age?'' A study commissioned by the European Commission's Information Society and Media Directorate-General,(November 2009).

[52] For an overview of issues related to the E-Commerce Directive see: Commission Staff Working , Document, Online services, including e-commerce, in the Single Market, Brussels, 11.1.2012 SEC(2011)1641final, http://ec.europa.eu/internal_market/e-commerce/ .*available* at: https://www. jipitec.eu/issues/jipitec-8-3-2017/4623

[53] See more on the practice of designating corporate actors to enforce rules on the Internet in N. Tusikov, Chokepoints - Global Private Regulation on the Internet, University of California Press, November 2016.

content or activities, the States enlist the intermediaries to enforce the public policy objectives (i.e. to remove unlawful content).

European Commission Public meeting on the future of e-commerce the internal market and the implementation of the Directive on electronic commerce sets out essential necessities on obligatory consumer data and steps to be followed in internet contracting and rules on business correspondences, for example, online advertisement and unsolicited commercial communication.

Under Article 14 of the Directive, the decision to remove or disable access to content has to be expeditious in order to exonerate the service provider from the potential liability. The most cautionary approach is to act upon any indication of illegality, without engaging in any, possibly burdensome and lengthy, balancing of rights that may come into conflict. As a result, any investigation of the illicit character of the content and balancing of rights at stake is usually non-existent.[54] This often leads to instances of 'over-compliance' in case of takedown requests, or in other words, preventive over-blocking of entirely legitimate content. Article 14 of the E-Commerce Directive, therefore, creates "an incentive to systematically take down material, without hearing from the party whose material is removed".[55] The current legal situation has been characterised as an "inappropriate transfer of juridical authority to the private sector".[56] Others consider it a form of private or corporate censorship[57] possibly creating a 'chilling effect' on the right to freedom of expression. Service providers are placed under such fear of liability claims that they impose on themselves measures "appropriate for

[54] See discussion in C. Ahlert, C. Marsden and C. Yung, "How Liberty Disappeared from Cyberspace: the Mystery Shopper Tests Internet Content Self-Regulation" ("Mystery Shopper") at: http://www.rootsecure.net/content/downloads

[55]. R. J. Barceló and K. Koelman, "Intermediary Liability In The E-Commerce Directive: So Far So Good, But It's Not Enough'', Computer Law & Security Report 2000, 231(vol. 4,2000).

[56] European Commission, Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (n 10) p. 12.

[57] R. J. Barceló, On-line intermediary liability issues: comparing EU and US legal frameworks, E.I.P.R. 2000, 111; The Organization for Security and Co-Operation in Europe and Reporters Sans Frontiers, Joint declaration on guaranteeing media freedom on the Internet, *available at* http://www.osce.org (last visited on June 7, 2020)

making themselves immune to any subsequent accusation but is of a kind that threatens the freedom of expression of Internet users”. [58]

Ecommerce Europe is an association which has played a pivotal role representing over 1 lakh companies selling products and services online to shoppers across Europe. Ecommerce Europe is presently the sole voice of the European Digital Commerce and represents web-based businesses. It acts to assist administrators across Europe with structuring a superior system for online traders in order to facilitate e-commerce and to help deals come through. presently the sole voice of the European Digital Commerce and represent web-based businesses. It acts to assist administrators across Europe with structuring a superior system for online traders in order to facilitate e-commerce and to help deals come through.

4.7.1 Report on the Application of the European Union Directive, 2003

Article 21 of the Directive 2000/31/EC provides that in 2003 and thereafter, every 2 years, the Commission shall provide the EU Parliament, the Council and also the Economic and Social Committee a report on the compliance of the Directive accompanied, wherever necessary, by proposals for adapting it to legal, technical and economic developments within the field.

The report provides the first assessment of the transposition and application of the Directive and its impact. The report is the first stage in a continuous process to ensure that Europe stays in the frontline of development in electronic commerce with a maximum level of legal certainty both for business and consumers**.**

4.7.2 European Commission Study on Directives 2012

On 11 January 2012, the European Commission received the Communication on electronic commerce and other digital services. In light of a

[58] E. Montero and Q. Van Enis, “Enabling freedom of expression in light of filtering measures imposed on Internet intermediaries: Squaring the circle’’, Computer Law & Security Review , 21-35 ((2011)

top to bottom public consultation. This Communication sets out the Commission's vision for the potential described by digital services in development and business, distinguishes the important snags in order to improve e-commerce and online services and thereby establish 5 priorities, accompanied by an action plan.

The Communication is accompanied by two staff working papers. The first working paper titled 'Online services, including e-commerce, in the Single Market' conducts an analysis of the factors hindering the development of e-commerce and serves as an application report in the light of Article 21 of the E-Commerce Directive. The second working paper entitled 'Bringing e-commerce benefits to consumers' presents a detailed analysis of the particular obstacles that have been identified as especially relevant for e-commerce in products.[59]

4.7.3 Report on the Implementation of the E-commerce of the E-commerce Action Plan, 2013[60]

The Commission published a report on progress made in the implementation of the e-commerce action plan. The report indicates that many important actions envisaged in the action plan have already been initiated:

a. reinforcing consumer protection by adoption of the "consumer agenda", development of tools for administrative cooperation and better enforcement of European Union law;

b. improving parcel delivery and payments (launch of public consultations);

c. fighting abuse (establishment of the European Cybercrime Center and definition of a cyber-security strategy);

---

[59] Ecommerce directive what happened and its adoption, *available* at https://ec.europa.eu/digital-single-market/en/news/archive-e-commerce-directive-what-happened-and-its-adoption (last visited on June 7,2020)

[60] *Ibid*

d. integrating technological developments (cloud computing strategy, Communication on radio spectrum sharing, guidelines on state aids on broadband, etc.).

In April 2018, the Commission also proposed a new deal for Consumers which will further strengthen Consumer rights online:

- Online commercial centres should advise customers whether they are purchasing from a merchant or a private individual, so they know about their privileges if something in turn goes wrong.
- At the point when consumers search on the web, they will be unmistakably educated about a query output being paid for by a trader and the digital market place should advise on the fundamental parameters deciding the positioning of the outcomes.
- At the point when customers pay for e-commerce service, they will profit by certain information rights with 14 days to drop the agreement.

4.8. Anticybersquatting Consumer Protection Act, 1999

The Anti-Cyber Consumer Protection Act (ACPA), is a law of the United States promulgated in 1999 which protects the e-consumer and e-business and established a cause of action for registering, or illegal trafficking in or using a fake domain name or diluting a brand or a person's name. The law was designed to thwart "cybersquatters" who register Internet domain names that contain trademarks without intending to create a legitimate website but instead plan to sell the domain name to the trademark owner or to a third party.[61]

In Harrison v. Microfinancial Inc.[62], ACPA has been used to successfully combat a consumer reprimand site. There, the court found that a discontented customer had violated the ACPA by registering a domain name containing the defendant's trademark, on which he ran a website that criticized

---

[61] Anticybersquatting Consumer Protection Act , *available* at https://en.wikipedia.org last visited on March 27,2020)

[62] 2005 USDistLexis 2804 (D. Mass., Feb. 24, 2005)

the accused. The jury finding bad faith concluded that it was largely based on the determination that the plaintiff had offered to transfer ownership to the accused if he had reimbursed some lease payments that the plaintiff had made and that were at the heart of his dispute with the defendant, as well as the applicant's funds which he claimed that the accused received unduly from third parties.[63]

The ACPA renders one at risk to the proprietor of a trademark who, with "a dishonest aim to benefit from that mark," "registers, traffics in or uses a domain name" that is either indistinguishable or confusingly comparable to a "distinctive" mark or is identical, confusingly similar or dilutive of a "famous mark".

If a violation of the ACPA is found, a court can "order the forfeiture or cancellation of the [offending] domain name or [its] transfer to the owner of the mark" (§1125(D)(1)(c)). The mark owner can also recover up to three times his actual damages and obtain injunctive relief. Actual damages include the profits which the domain name registrant made from his use of the mark, as well as losses sustained by the mark holder as a result of the domain name registrant's actions, such as lost sales or harm to the mark's reputation. In lieu of actual damages, the mark owner can elect to recover statutory damages of between $1,000 and $100,000 per domain (§1117). The actual amount awarded is fixed by the court in its own discretion (§1117(d)). In "exceptional cases", attorney's fees can also be recovered (§1117).[64]

4.8.1 'Cybersquatting' under ACPA

Cybersquatting occurs when someone registers a domain name in bad faith with the intent to financially benefit from a trademark that does not

[63] The Anticybersquatting Consumer Protection Act: Key Information, *available* at www.internetlibrary.com, (last visited on June 7,2021)
[64] *Id.* at 60.

belong to them. This can lead to a domain dispute between the owner of the trademark and the owner of the domain.[65]

The ACPA has been effectively used to combat a number of wrongs. These include “cybersquatting”, which occurs when a registrant obtains a domain name containing another’s mark and offers to sell it to the mark holder for a tidy sum. The ACPA has also been used to prevent domain registrants from improperly profiting from the commercial use of another’s mark, such as by selling or displaying ads for products that compete with those of the mark holder at a domain containing the mark. The ACPA has also been successfully used to prevent the tarnishing of a mark by its use in the domain of a website containing pornographic or other materials with which the mark holder does not wish his mark associated. In addition, the ACPA has been used to combat websites critical of the mark holder set up at a domain containing his mark.[66]

The Anticybersquatting Consumer Protection Act provides remedies including the transfer of a domain name if there is bad faith intent to profit from that mark, by a cybersquatter who registers, traffics in, or uses a domain name that is identical or confusingly similar to a distinctive or famous mark.

Legal action under the Anticybesquatting Consumer Protection Act (ACPA). To have a successful case under the ACPA, a trademark owner must prove each of the following:

- The registrant had offensive intention to benefit
- the trademark was unique prior to the date the domain name was first registered
- The domain name is either identical or confusingly like the trademark
- The owner was the first to use the unique trademark

---

[65] What is cybersquatting and how can it affect trademark, *available* at https://igerent.com/what-cybersquatting-and-how-can-it-affect-trademark (last visited on March 20,2019)

[66] Anticybsquatt, *available* at http://www.internetlibrary.com/publications/anticybsquattSamson9-05_art.cfm (last visited on March 20,2019)

4.9. The Organisation for Economic Co-operation and Development[67]

The Organisation for Economic Co-operation and Development (OECD) grew out of the organisation for European Economic Cooperation, which administered American and Canadian aid to Europe after World War II. Established in 1961, OECD today has 36 member countries in 2019. Its goals are to build strong economies in its member countries, improve market systems, expand free trade and contribute to development in both developed and developing countries. The governing body of OECD, the Council, is led by a secretary-general and is made up of representatives of member countries, who provide guidance on the work of OECD committees and decide on the annual budget.

4.9.1. OCED and E-Commerce

E-commerce has become an area of focus for OECD because of its cross-border nature and its potential for all countries in the areas of economic growth, trade and improved social conditions. It has developed policy in areas ranging from telecommunication infrastructure and services to taxation, consumer protection, network security, privacy and data protection, as well as emerging markets and developing economies.

Following its “OECD Action Plan for Electronic Commerce”, endorsed by its members in 1998, it’s ‘work programme’ focuses to build trust for users and consumers; establishes ground rules for the digital marketplace; enhance the information infrastructure for e-commerce; and maximize the benefits of e-commerce. Some of the activities currently under way in the area of e-commerce include:

- implementing aspects of the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce;

[67] The organisation for Economic Co-operation and Development, *available* at http://www.oecd.org (last visited on March 20,2019)

- promoting the use of privacy-enhancing technologies and user education and awareness about online privacy issues;
- studying the effects of e-commerce on cross-border trade in financial services, on contract law and on electronic delivery of insurance products;
- studying access to high-bandwidth information and communication technologies at affordable costs in rural as well as in urban areas;
- researching the needs and constraints of capacity development for trade faced by developing countries; and
- disseminating its work on e-commerce to member and non-member countries through other international organizations.

4.10 The Hague Conference, 1995

The Hague Conference is an intergovernmental association that attempts to bind together private international law rules. The first, meeting of the Hague Conference was held in 1893; after seven additional sessions, a statute came into force in 1955 making the Conference a permanent association.

The main role of the Conference is to negotiate and draft multilateral treaties (conventions) in the different fields of private international law. The Hague Conference areas of concern include:

- maintenance (support) obligations.
- applicable law and international judicial and administrative cooperation regarding civil liability for environmental damage;
- problems of private international law raised by electronic interchange;
- conflict of jurisdictions;

4.10.1 The Hague Conference and E-Commerce

In 1999, the Conference held a round-table conversation (related to the University of Geneva) with specialists from different fields on issues emerging from e-commerce and Internet exchanges. A progression of suggestions were embraced in such areas as online agreements, B2B and B2C exchanges and online dispute resolutions. In June 2001, the Conference held its Nineteenth Session and progressed in the direction of the Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters and to choose its future work program. Delegates based their debates on both a Preliminary Draft of the Convention as drawn up in October 1999 and on the results of formal and casual meetings of experts on e-commerce and intellectual property.

4.11. WTO Working Programme on E-Commerce

At the Second Ministerial Conference in May 1998, ministers, recognizing that global electronic commerce was growing and creating new opportunities for trade and therefore adopted the Declaration on Global Electronic Commerce. This called for the establishment of a work programme on e-commerce, which was adopted in September 1998. Periodic reviews of the programme are conducted by the General Council based on reports from the WTO bodies responsible for implementing the programme. Ministers also regularly consider the programme at the WTO's ministerial conferences.[68]

4.11.1. Background

The Declaration instructed the General Council to establish a comprehensive work programme to examine all trade-related issues relating to global electronic commerce, including issues identified by Members. Ministers also declared that Members will continue their practice of not imposing customs duties on electronic transmissions ("moratorium" on customs duties). The Secretariat issued a Note to assist Members in their deliberations on trade-

[68]Electronic Commerce Gateway, *available* at https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm (last visited on March20, 2019)

related issues pertaining to global electronic commerce pursuant to the Ministerial Declaration on Global Electronic Commerce.[69]

In September 1998, the General Council adopted the Work Programme on Electronic Commerce.

4.11.2. Definition of Electronic Commerce

The Work Programme on Electronic Commerce states that "exclusively for the purposes of the work programme, and without prejudice to its outcome, the term 'electronic commerce' is understood to mean the production, distribution, marketing, sale or delivery of goods and services by electronic means". Four WTO bodies were charged with the responsibility of carrying out the Work Programme: the Council for Trade in Services; the Council for Trade in Goods; the Council for TRIPS; and the Committee on Trade and Development. The General Council plays a central role and keeps the work programme under continuous review.

The Work Programme on Electronic Commerce instructed:

- the Council for Trade in Services to analyze and report on the treatment of electronic commerce in the GATS lawful system;
- the Council for Trade in Goods to examine to look at and report on characters of digital commerce important to the provisions of GATT[70] 1994,
- the multilateral trade agreements secured under Annex 1A of the WTO Agreement, and the approved work*programme;
- the Council for TRIPS to analyze and report on the intellectual property issues regarding electronic commerce;

[69] *Id.* at 56.
[70] The General Agreement on Tariffs and Trade (**GATT**) is a legal agreement between many countries, whose overall purpose was to promote international trade by reducing or eliminating trade barriers such as tariffs or quotas.

The Committee on Trade and Development to examine and report on the development implications of electronic commerce, taking into account the economic, financial and development needs of developing countries.

Since May 2001, the General Council's assessment of cross-cutting issues under the Work Program has been done in dedicated conversations held for this reason. The first Dedicated Discussion was held on 15 June 2001 under the sponsorship of the General Council. Following that gathering, the Secretariat circulated a summary of the issues raised and a list of cross-cutting issues distinguished by delegations of member countries. The twelfth and most recent Dedicated Discussion was held on 18 October 2016. Since then, discussions have continued in informal, open-ended meetings convened by the General Council Chair and through the review of progress in the General Council.[71]

4.11.3. Ministerial Decisions on the Work Programme on Electronic Commerce

Ministers have considered the Work Programme on Electronic Commerce Ministers at their Ministerial Conferences in Geneva (1998), Doha (2001); Hong Kong (2005); Geneva in (2009); Geneva (2011) and Bali (2013). At these Conferences, Ministers have observed the reports on electronic commerce and have instructed the General Council and its relevant bodies to proceed with their work on e-commerce. Ministers have additionally consented to proceed with the act of not forcing customs obligations on electronic transmissions until their next meeting.

WTO members meeting as the General Council concurred on 10 December 2019 to extend two existing moratoriums identified with customs duties on electronic commerce and the inception of "non-violation" complaints

[71]WTO | Trade Topics - Electronic commerce - Work programme, *available at* www.wto.org/english/tratop_e/ecom_e/ecom_e.htm ,(last visited on March 20,2019)

under the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). They additionally endorsed the WTO's budget for 2020.[72]

4.12. E-commerce Law in Singapore

In Singapore, the Electronic Transactions Act (ETA) regulates electronic commerce transactions. It was first adopted in July 1998 to provide a legal basis for electronic signatures. Singapore is one of the first countries in the world to pass a legislation which deals with the problems that may arise in the context of electronic contracts and digital signatures. It deals with the responsibility of network service providers and the formation and validity of electronic contracts,[73] based on the UNCITRAL model laws. It solves the problem of managing the contract in traditional form even in case of electronic commerce. It will also help us to resolve the problem of uncertainty in electronic contract laws. In addition, the law also clarifies the position of electronic contracts. In this part, the validity or the applicability cannot be denied although the offer and the acceptance are done through electronic registrations. The law lists the requirements for issuing, suspending and revoking a certificate and establishes the obligations of subscribers under the law. Finally, the law appoints the controller of the certification authorities and authorizes the government to accept and publish electronic documents.[74]

4.12.1. Electronic Transactions (Certification Authority) Regulations, 1999

The regulations govern the actions of the certification authorities in Singapore. They refer to the application procedures, including rights and financial criteria, as well as to the renewal and duration of a license. In addition, certification authorities are subject to compliance audits and must keep reliable records of their transactions. The regulations also define the types

[72] *Available* at https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm,(last visited on March20,2019)

[73] Francis O A, "Analysis of Electronic Transactions Bill in Nigeria': Issues and Prospects'' *Mediterranean Journal of Social Sciences* ISSN 2039-9340 (vol 5, No 2 January 2014)

[74]Baker, McKenzie "Singapore E-Commerce Legislation and Regulations' http://www.bakermckenzie.com (last visited on December 12, 2018)

of certificates and the requirements for the issue, renewal, suspension and revocation of certificates. The regulations recognise repositories as well as secure digital signatures and the formation of an electronic contract.[75]

4.12.2 Information Technology Security Guidelines

IT guidelines on security should be used by organizations in their struggles to develop and implement their cyber security programs. They provide a set of basic guidelines on which an organization can build its organization-specific policies and guidelines. The main topics covered by these guidelines are as below:

i) Security of IT management
ii) Management of digital information
iii) Personnel and organizational security
iv) Security controls and system integrity
v) Operational security and physical
vi) Security of network and communication
vii) LAN and workstation security and distributed system
viii) E-commerce plays a vital role in Singapore economy as it provides business and economic advantages through the creation of new growth channels.

The Singapore Government recognizes this growth potential and is keen to invest in innovation by local firms, as well as to assist them in rethinking their growth strategies.

Singapore has become a successful e-commerce hub with many international companies placing their e-commerce operations in Singapore. Rakuten from Japan and Taobao from China, both are online marketplaces that have set up their regional offices in Singapore in order to adjust sales and operations in South East Asia. These foreign e-commerce players cite

[75] Developing_Legal_framework_for_ecommerce in Nigeria Lessons from UK and Singapore., *available at* https://s3.amazonaws.com/academia.edu. (last visited on December 10, 2018)

Singapore's strong IT infrastructure, great level of digital adoption, entrepreneurial climate and contiguity to neighbouring countries as the major factors that make Singapore an ideal tested location to design and launch new e-Commerce goods and services before rolling them out in the region.[76]

4.13. United Nations Guidelines for Consumer Protection (UNGCP)

The UNGCP was adopted with consensus in 1985 and follows on account of a long campaign by consumer associations in many countries with Consumers International (then known as the International Organization of Consumer Unions since its creation in 1960 and with more general consultative status by the Economic and Social Committee) in 1977 after the United Nations. The United Nations, at its 1975 World Congress in Sydney, was invited to develop a "Model Code for Consumer Protection". Because of which, the ECOSOC[77] instructed the Secretary-General in 1977 to prepare a survey of national institutions and legislation in the field of consumer protection, and in 1981 ECOSOC asked the Secretary-General to continue consultations on protection consumers to develop a set of general guidelines for consumer protection, in particular taking into account the needs of developing countries.

The draft guidelines were sent to governments for comments in 1982 and submitted to ECOSOC in 1983. Many sources were used, including the OECD, the United States' Bill of Rights for Consumers, and several agency materials from consumer protection authorities and consumer associations.[78]

The guidelines were adopted for the first time by the General Assembly in its resolution 39/248 of 16 April 1985, then extended by the Economic and Social Council (ECOSOC) in the resolution E / 1999 / INF / 2 / Add.2 of 26

[76] *Id*. at 62.

[77] United Nations Economic and Social Council (ECOSOC) is responsible for coordinating the economic, social and related work of UN specialized agencies, their functional commissions and regional commissions.

[78] United Nations Guidelines for Consumer Protection, *available at* https://en.wikipedia.org (last visited on March 27,2020)

July 1999 and resolution 70/186 of 22 December 2015, as revised and amended by the General Assembly.

The revised UNGCP 2015 is preceded by the General Assembly resolution 70/186 on consumer protection, which specifically addresses the needs of developing countries vis-à-vis the Sustainable Development Goals as successors to the Millennium Development Goals and the need for governments to work together across borders. Reference to changes since 1999 are included in the paragraphs on data protection, e-commerce and financial services, as an express answer to the recent financial crisis and disturbances in the digital economy. The last two developments are the subject of new sections in the guidelines. The Intergovernmental group of experts on consumer protection law and policy should continue under the existing UNCTAD mechanisms in parallel with the further review of "all United Nations competition".[79]

4.13.1 Objectives of UNGCP

Taking into account the interests and requirements of consumers across all nations, particularly developing countries, it is important to recognize that consumers often face inequalities in economic terms, education levels and bargaining power. Furthermore, while taking into account the rights of consumers to have access to non-hazardous products, as well as the importance of promoting equitable and sustainable economic conditions and social development, these consumer protection guidelines have the following objectives:

- Help countries to ensure or maintain adequate protection of their populations as consumers;
- Facilitate production and distribution models that meet the needs and desires of consumers;

[79] *Id.* at 65.

- To give a high level of moral and ethical conduct for those who engaged in the production and distribution of services and goods to consumers;
- Help countries to reduce the abusive business practices of all companies at the national and international levels which have a negative impact on consumers;
- Facilitate the development of independent consumer groups;
- Promote global cooperation in the area of consumer protection;
- Encourage the development of market conditions that offer consumers more choices at lower prices.

4.13.2 General principles of UNGCP[80]

- Countries should develop, establish or maintain a strong consumer protection policy worldwide, taking into account the guidelines set out below. In doing so, each government must set its own consumer protection priorities based on the economic and social situation of the country, taking into account the needs of its people and the costs and benefits of the measures proposed.
- The legitimate requirements for which the guidelines are intended to be met are:
  a) Protect consumers from dangers to their health and safety;
  b) Promote and protect the commercial interests of consumers;
  c) Access by consumers to sufficient information to enable them to make informed choices based on individual wishes and needs;
  d) Consumer education;
  e) Availability of effective consumer satisfaction;
  f) The freedom to train consumers or other groups or organizations concerned and the possibility for these organizations to present their points of view in the decision-making processes which affect them

[80] Consumer protection, *available at* http://hrlibrary.umn.edu/links .html , (last visited on March 27,2020)

- Governments must provide or manage the adequate infrastructure to develop, implement and monitor consumer protection plans. Particular attention should be paid to ensuring that consumer protection measures are implemented for the benefit of all sectors of the population, especially the rural population.
- All companies must comply with the relevant laws and regulations of the countries in which they operate. They should also comply with the appropriate provisions of the International Consumer Protection Rules, which have been registered by the competent authorities of the country. (Reference to international standards in the guidelines should be considered in the context of this section.)
- The potential positive role of universities and public and private companies in research should be taken into account in the development of consumer protection policy.
- Government should establish consumer protection policies that provide clear and timely information to allow consumers to contact the business easily, and to allow law enforcement and regulation authorities to identify and locate them. This may include information such as the identity of the company, its corporate name and the name with which it trades, its main geographical address, its website, and its e-mail address or any other means of contact, its telephone number its contact, information, and government registration.
- Ensure that consumer protection enforcement agencies have the human and financial resources necessary to promote effective compliance and to obtain or facilitate consumer redress in an appropriate case.
- The UN International community must adopt or maintain policies to ascertain manufacturer's liability, to ensure that the durability of goods, utility and reliability requirements are met and that they are suitable for the purpose for which they are intended and that the seller must guarantee that these requirements are met. Similar policies should be provided with regards to services as well.

- The international community should adopt or formulate or promote the development and implementation of appropriate standards for goods and services, at the national and international levels, for the safety and quality of goods and services and give them adequate publicity. National standards and regulations for product safety and quality should be periodically reviewed to ensure they conform, if possible, to generally accepted international standards.
- The international community should encourage consumer organizations and other interested groups, including the media, to undertake education and information programs, including the environmental impact of consumption patterns and the possible implications, including the pros and cons, the associated cost of changes in consumption, especially for the benefit of low-income consumer groups in rural and urban areas.
- Responsibility for sustainable consumption is to be shared by all members and organizations of society, through informed consumers, Member States, companies, labour organizations and consumer and environmental organizations which will play a particularly important role. Informed consumers play an essential role in promoting environmentally, economically and socially sustainable consumption, including the impact of their choice on producers. Member States should promote the development and implementation of sustainable consumption policies and the integration of these policies with other public policies.
- Policy development by the member countries should be done in consultation with business, consumer and environmental organizations and other engaged groups. Business groups are particularly to be made responsible for promoting sustainable consumption through the design, production and distribution of services and goods. Consumer and environmental organizations have a responsibility to promote public participation and debate on sustainable consumption, to further inform other consumers and to work with international communities and businesses on sustainable consumption.

- The international community should strive to build consumer confidence in e-commerce by continually developing transparent and effective consumer protection policies, ensuring a level of protection not lower than that offered in other forms of trade. The international community should, where appropriate, review existing policies.
- Consumer protection policies to take account of the peculiarities of e-commerce and ensure that consumers and businesses are informed and aware of their rights and duties in the digital market.
- The international community may wish to consider relevant international e-commerce guidelines and standards and their amendments and, where appropriate, adapt those guidelines and standards to their economic, social and environmental conditions so that they may comply with them and across the boundaries and cooperate with other international communities in their implementation. Thus, the international community may want to study the consumer protection guidelines in the context of e-commerce of the Organization for Economic Cooperation and Development.
- The international community should improve its capacity to cooperate in the fight against fraudulent and deceptive cross-border business practices, as this serves public interest. However, recognizing that cooperation in the context of investigations or specific cases falling under these guidelines remains yet to be seen.
- The international community should consider participating in multilateral and bilateral agreements to improve international judicial and inter-agency cooperation in the recovery of foreign activities and in the enforcement of judgments in cross-border cases.
- To educate consumers and the develop information programs for them they should cover these important aspects with regards to consumer protection:

a) Health, nutrition, prevention of foodborne illnesses and food forgery;
b) Hazardous products;
c) Labelling of products;

d) Relevant law and policy, how to obtain redress, and agencies and organizations for consumer protection;

e) Information about weights and measures, prices, quality of goods and services, credit conditions and availability of basic necessities; and

f) As relevant, pollution and the environment.

- In promoting the interests of consumers, particularly in developing countries, governments should prioritize areas of concern for consumers' health, such as food, water and pharmaceuticals, wherever appropriate. Policies should be adopted or maintained for product information and quality control, as well as education and research programs in these areas. Government guidelines should be developed for specific areas with reference to the provisions of such documents.
- When formulating national food policies and plans, governments should take into account the food safety needs of all consumers and, where possible, support and adopt UN standards, The World Agricultural and Health Organization Codex Elementris[81] or, in their absence, others generally accept international food standards. Governments must maintain, develop or improve food safety measures, including food safety standards, food standards and dietary requirements and effective monitoring, inspection and evaluation mechanisms.
- Governments should, within the framework of the goals and objectives set for the International Decade of Drinking Water Supply and Sanitation, formulate, maintain or strengthen national policies to improve the supply, distribution and quality of drinking water. It is necessary to take into due consideration the choice of adequate levels of service, quality and technology, the need for educational programs and the importance of community participation.

---

[81] The Codex Alimentarius, or "Food Code" is a collection of standards, guidelines and codes of practice adopted by the Codex Alimentarius Commission. Codex has worked since 1963 to create harmonized international food standards to protect the health of consumers and ensure fair trade practices.

- Governments should develop or maintain adequate standards, regulations, and regulatory systems to ensure the quality and proper use of medicines through integrated national drug policies, which could include, inter alia, supply, distribution, production, license agreements, systems registration and availability of reliable information on pharmaceutical products and services. In doing so, the government should pay particular attention to the work and recommendations of the World Health Organization (WHO) on pharmaceutical products. For relevant products, use the WHO's certification system to assess the quality of pharmaceutical products entering international trade, especially in case of pharmaceutical products which are to be administered to aged people. Measures should also be taken, where appropriate, to promote the use of international non-proprietary names (INNs)[82] for drugs, drawing on the work done by the World Health Organization.

- Governments should, in particular in a regional or sub regional context:

  a) Develop, review, maintain or, if necessary, strengthen information exchange mechanisms on national consumer protection strategies and measures;

  b) Cooperation or promotion of cooperation in the implementation of consumer protection standards in order to get better results with the available resources.

  c) Examples of such collaboration could include collaboration in setting up or sharing test facilities, shared testing procedures, sharing consumer information and educational programs.

  d) Cooperate to improve the conditions under which essential products are offered to consumers, taking due account of both price and quality. This cooperation could include the joint purchase of essential goods, the

[82] The international nonproprietary name (INN) is an official generic and non-proprietary name given to a pharmaceutical drug or an active ingredient. INNs make communication more precise by providing a unique standard name for each active ingredient, to avoid prescribing errors.

exchange of information on different procurement possibilities and agreements on regional product specifications.

- Given the need to reach rural consumers and the illiterate, governments should develop or promote the development of consumer information programs in the media, where appropriate.
- Governments should organize or promote educational programs for educators, mass media professionals and consumer advisers so that they can participate in the implementation of consumer information and education programs.

4.14. Conclusion

The most important feature of globalization has been the internet which has given rise to a new wave in the economy in the form of electronic commerce. Digital transactions are profoundly affecting the world economy, polity and society. Today an accepted fact that information and communication technologies can present itself as an opportunity, in particular for developing countries to dramatically improve their economics. First part of the chapter gives a broad description of ICT and discusses various tools and techniques of e-commerce. Smart phones, broadband, smart home devices and online shopping websites are a new trend in the growth of the e-commerce environment. E-commerce and new emerging digital technology and services can be real tools for development and help improve the livelihood of millions across the globe, by linking up remote regions and bringing together scientists, administrators, health professionals, managers, and people into projects and programmes to promote economic and social development. This window of opportunity that ICTs and e-commerce have given is available to all regions.

The success of electronic commerce will require a powerful partnership between the private and public sectors, with the private sector in the lead. Government participation must be coherent and cautious, avoiding the contradictions and confusion that can sometimes arise when different governmental agencies individually assert authority and operate without coordination.

Part second of the chapter deals with international legal framework including relevant conventions on electronic commerce. The WTO ministerial meeting held in DAVOS, Switzerland, on Jan 25, 2019, it is noteworthy that the members of the meeting were impatient with the lack of development in the World Trade Organization rules to cover the explosive growth of e-commerce. Therefore, 76 countries and regions agreed to start negotiating this year on a set of open and predictable regulations. The WTO's 164 members were unable to consolidate some separate e-commerce proposals at the body's biennial conference at Buenos Aires in December 2019, including a call it set up with central e-commerce negotiating forum. According to Japan's trade minister Hiroshige Seko, the current WTO rules don't match the needs of the 21st century since there are no solid rules on e-commerce and thus it seems that the WTO ministerial conference in December has failed to reach any new agreement. The stalemate dashed hopes for new ideals on regulating the widening presence of e-commerce.

The chapter has carried out a study on international law relating to e-commerce and consumer protection. It is well settled that e-commerce contributes immensely to the global economy. E-commerce can encourage the economy of any country to grow and expand, so far, the country wishes to take the advantages brought by the breakthrough in the modern-day information technology. However, this is not possible to be achieve without putting in place the relevant legal framework that will protect online consumers or e-consumers. The UN guidelines may play a great role in the field of law-making process at an international level but in the present situation, no country is ready to enforce another country's decision because each country has their own priorities, interests and infrastructure, etc. Taking an example of China which is a non-democratic country and has no freedom to press and media, will not allow the adoption of any international mechanism to his territory until and unless it is not beneficial for China.

In the next chapter, the researcher undertakes an in-depth study of the Indian legal framework pertaining to different legislations, directly and indirectly, regulating and pertaining to e-commerce and cyber offences. The chapter has a dual approach, in the first part it analysis the substantive and procedural laws pertaining to the realm of e-commerce and cyber laws. Whereas in the second aspect, the chapter discusses various judicial decisions which have helped shape the legal gamut pertaining to e-commerce, cybercrimes and the implementation of cyber laws and legislations pertaining thereto.

CHAPTER - 5

INDIAN LEGAL FRAMEWORK OF E-COMMERCE

CHAPTER - 5

INDIAN LEGAL FRAMEWORK OF E-COMMERCE

The previous chapter provided an in-depth analysis on the prevalent use of information and communication technologies (ICTs) and its importance and prominence in terms of global economic processes. It assessed these aspects of ICT as crucial indicators of various aspects of e-commerce, growing trends, economic development, etc. It also explored the various tools and techniques relating to ICT employed in this regard in order to advance growth and development in e-commerce sector. It further provides for an extensive study and analysis of the international legal framework on e-commerce and e-commerce related aspects.

In the present chapter, the researcher analyses the various legislations therein which provide an important insight into the existing legal framework pertaining, directly and indirectly, to e-commerce and cyber offences. The chapter analysis both substantive and procedural aspects of the law with regards to e-commerce and cyber laws and the recent amendments and legislations enacted to bring e-commerce and related cyber offences into the existing legal realm. The chapter further analyses the Indian judicial approach and studies various decisions pertaining to e-commerce, cybercrimes and the implementation of existing laws relating thereof.

Presently in India, e-commerce is developing at a high rate, however the conventional law does not provide solutions for problems pertaining to e-commerce. Thus, there is a need for separate and stringent laws to regulate it. This chapter is dedicated to deal with laws relating to electronic commerce and the limitations and barriers that e-commerce presently faces in the digital era.

In the Indian scenario, it can be said that the Information Technology Act, 2000 (IT Act) attempts to solve some of the issues specific to information and authentication of electronic commerce. The IT Act has brought about changes to various enactments, such as the Indian Evidence Act, Indian Penal Code, Criminal Procedure Code, Reserve Bank of India Act, to name a few.

The IT Act essentially seeks to address three areas of perceived requirements for digital commerce:

- To make possible e-commerce transactions
- To make possible e-governance transactions
- To curb cybercrime and regulate the internet.

5.1. Information Technology Act, 2000

5.1.1 Preamble

The Preamble of the IT Act, 2000, states that it is an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as ‘electronic commerce’. This may include the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies. Further, the IT Act will seek to amend the Indian Penal Code, the Indian Evidence Act, the Banker’s Books Evidence Act, and the Reserve Bank of India, for related matters.

The Act, as laid down in the Preamble, also follows closely the Model Law on Electronic Commerce adopted by the UNCITRAL. The aforementioned Model Law recommends that all States give favorable consideration to the said Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information. Moreover, it has been stipulated that the said resolution may be given effect to efficient delivery of Government services accomplished, by means of reliable electronic records. The Model Law provides a starting point for identification and discussion of areas where the law could be updated, taking into consideration new technology, as well as including certain internationally accepted provisions for the following issues:

- Establish rules that validate and recognize e-commerce formed through electronic means;
- Sets default rules for e-commerce and governance of electronic commerce performance;
- Defines the characteristics of a valid writing and an original document;
- Provides for the recognition of electronic signatures for a legal and commercial purpose; and
- Supports the admission of computer evidence in courts and arbitration proceedings.

5.1.2. Structure

The IT Act consists of 94 clauses divided into XIII chapters, of which the first 17 sections are largely based on the UNCITRAL Model Law. Furthermore, it has four schedules, of which Schedule I seeks to amend the Indian Penal Code; Schedule II seeks to amend the Indian Evidence Act; Schedule III seeks to amend the Banker's Books Evidence Act, and Schedule IV seeks to amend the Reserve Bank of India Act. Fourteen provisions specifically deal with some or the other aspect of digital signatures. Nineteen provisions pertain to private certifying authorities which will be licensed to issue digital signature certificates and the Controller, Deputy Controller and Assistant Controller who will be public servants, licensing and supervising the work of the certifying authorities.

Sections 65 to 79 of the IT Act set out the offences which will result in criminal liability which may entail imprisonment and/or fine, while Sections 43, 44 and 45 of the IT Act provide for penalties and compensation to be adjudicated by the adjudicating officers [Sections 46 and 47]. Appeals against the orders of the adjudicating authorities are to be made to the Cyber Regulations Appellate Tribunal and thereafter to the High Court. Section 48 to 64 of the IT Act deal with the Tribunal, appeals to the High Court and the compounding of the offences under this law.

The IT Act deals with the concepts of electronic governance, digital signatures, digital signature certificates, electronic records and regulation of certifying authorities and will go a long way in facilitating and regulating e-commerce. Furthermore, additional guidelines on internet-based trading and services have been prescribed.

5.1.3. Relevant Provisions Governing E-Commerce

5.1.3.1 Electronic Signatures

Electronic or Digital Signatures consist of cryptographic techniques which ensure privacy and verify the origin and integrity of the message; the techniques commonly used are a mix of algorithms, keys and codes. Symmetric cryptography uses just a single key to encrypt and decrypt the messages, on the other hand, asymmetric technique uses two keys one of which is public (because it is known by the parties) and one, which is private (just one of the parties knows it). Most modern signatures are based on asymmetric methods, described as a special door that can only be opened with four key lock, two on either side. Once both parties have locked the keys into the door, it is possible to open the door and for the parties to be sure that they can negotiate through that open door safely.[1] Signatures serve the purposes of evidence,[2] approval,[3] efficiency and logistics.[4] Further, a new section 3A was inserted in the IT (Amendment) Act, 2008 and

[1] Joga Rao, *Computer Contracts and Information Technology Law*, 2nd Ed., Vol. 1, Wadhwa & Co.,Nagpur, 2005 p. 57
[2] A signature authenticates writing by identifying the signer with the signed document. When the signer makes distinctive mark it becomes attributable to the signer; cited by Alwyn Didar Singh, *E-Commerce in India: Assessments and Strategies for the Developing World.*
[3] A signature expresses the signer‘s approval or authorization of the writing, or his intention that the document has legal effect;
[4] A signature on a written document imparts a sense of clarity and finality; cited by *Id.* at. *3.*

digital signatures were substituted with ‘electronic signatures’. Section 3A provides for Electronic Signature as follows:

1) Notwithstanding anything contained in Section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which:
   - **a)** is considered reliable; and
   - **b)** may be specified in the Second Schedule.
2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if:
   - **a)** the signature creation data or the authentication data were at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
   - **b)** any alteration to the electronic signature made after affixing such signature is detectable;
   - **c)** any alteration to the information made after its authentication by electronic signature is detectable; and
   - **d)** it fulfils such other conditions which may be prescribed.
3) The Central Government may prescribe the procedure for the purpose of ascertaining whether an electronic signature is that the person by whom it is purported to have been affixed or authenticated.
4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure

for affixing such signature from the Second Schedule: Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.

5.1.3.2 Privacy

While finishing the digital transactions, a number of individual data is obtained for example consumer's character, choice, details about the family, banking information related data, etc. Due to this, there are two essential privacy concerns, unauthorized access and abuse of individual data. Privacy was additionally considered under the IT (Amendment) Act 2008 and provisions were chalked out relating to punishment for violation of privacy. As sensitive data like passwords, individual details and so on are kept on servers of e-commerce business organizations; the security of such data gets significant. These security dangers can be outside the organisation (from hackers, infections and Trojan ponies) or from within the organizations, their staff, and workers). The IT Act 2000 deals with the issue of hacking with PC framework in Section 66 and Section 65 particularly deals with altering PC source records. Section 66 was amended in the IT (Amendment) Act 2008 to address PC related offenses, however, the issue of time framework security was not satisfactorily tended to.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011 provides for recording security practices and norms and recommends comprehensive documented data security program and information security approaches that contain administrative, specialized, operational and physical security control measures that ensure the protection of data resources as per the nature of business.

5.1.3.3 Attribution of Electronic Records

'Electronic record' means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.[5] Section 11 of the IT Act mandates that the electronic record in the given context is required to be attributed to the originator:

1) If the electronic record was sent by the originator himself or herself; or
2) If the electronic record sent by a person who was authorized by the originator to act so with regard to a specific record; or
3) By a computer system which was programmed either by the originator or by any person who is authorized to do so to operate automatically or otherwise.

[5] The Information Technology Act, 2000 (Act 21 of 2000), s. 2(t)

5.1.3.4 Offences and Penalties

Section 65 to Section 74 describes various offences and prescribes penalties for such offences. The relevant provisions are provided herein below:

Section	Offence	Punishments	Nature
Section 65	Tampering with Computer Source Code	Imprisonment upto 3 years or fine upto Rs. 2 lakhs	The offence is bailable, cognizable and triable by court of Judicial Magistrate First Class (JMFC).
Section 66	Computer Related Offences	Imprisonment upto 3 years or fine upto Rs. 5 lakhs	Offence is bailable, cognizable and triable by court of JMFC
Section 66-A	Sending offensive messages through Communication service, etc.	Imprisonment upto 3 years and fine	Offence is bailable, cognizable and triable by court of JMFC
Section 66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment upto 3 years and/or fine upto Rs. 1 lakhs	Offence is bailable, cognizable and triable by court of JMFC
Section 66-C	Identity Theft	Imprisonment of either description upto 3 years and/or fine upt Rs. 1 lakhs	Offence is bailable, cognizable and triable by court of JMFC
Section 66-D	Cheating by Personation by using computer resource	Imprisonment of either description upto 3 years and /or fine upto Rs. 1 lakhs	The offence is bailable, cognizable and triable by court of JMFC
Section 66-E	Violation of Privacy	Imprisonment upto 3 years and /or fine upto Rs. 2 lakhs	Offence is bailable, cognizable and triable by court of JMFC
Section 66-F	Cyber Terrorism	Imprisonment extend to	The offence is Non-Bailable, Cognizable

		imprisonment for life	and triable by court of Sessions
Section 67	Publishing or transmitting obscene material in electronic form	On first conviction imprisonment upto 3 ears and/or fine upto Rs. 5 lakhs On Subsequent conviction imprisonment upto 5 years and/or fine upto Rs. 10 lakhs	Offence is bailable, cognizable and triable by court of JMFC
Section 67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment upto 5 years and/or fine upto Rs. 10 lakhs On subsequent conviction imprisonment upto 7 years and/or fine upto Rs. 10 lakhs	Offence is non-bailable, cognizable and triable by court of JMFC
Section 67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first conviction imprisonment of either description upto 5 years and/or fine upto Rs. 10 lakhs On Subsequent Conviction imprisonment of either description upto 7 years and/or fine upto Rs. 10 lakhs	Offence is non-bailable, cognizable and triable by Court of JMFC
Section 67-C	Intermediary intentionally or knowingly contravening the directions about preservation and retention of information	Imprisonment upto 3 years and fine	Offence is bailable, cognizable.
Section 68	Failure to comply with the	Imprisonment upto 2 years and/or	Offence is bailable, non-cognizable.

	directions given by Controller	fine upto Rs. 1 lakh	
Section 69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment upto 7 years and fine	Offence is non-bailable and cognizable.
Section 69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment upto 7 years and fine	Offence is non-bailable and cognizable
Section 69-B	An intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard to monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment upto 3 years and fine	Offence is bailable, cognizable.
Section 70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description upto 10 years and fine	Offence is non-bailable, cognizable.

Section 70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres etc.. who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment upto 1 year and/or fine upto Rs. 1 lakh	Offence is bailable, non-cognizable.
Section 71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment upto 2 years and/ or fine upto Rs. 1 lakh.	Offence is bailable, non-cognizable.
Section 72	Breach of confidentiality and privacy	Imprisonment upto 2 years and/or fine upto Rs. 1 lakh.	Offence is bailable, non-cognizable.
Section 72-A	Disclosure of information in breach of lawful contract	Imprisonment upto 3 years and/or fine upto Rs. 5 lakh.	Offence is bailable, non-cognizable.
Section 73	publishing electronic signature certificate false in certain particulars	Imprisonment upto 2 years and/or fine upto Rs. 1 lakh	Offence is bailable, non-cognizable.
Section 74	Publication for fraudulent purpose	Imprisonment upto 2 years and/or fine upto Rs. 1 lakh	Offence is bailable, non-cognizable.

According to Section 77-B of the Act, the offences punishable with imprisonment of three years and above shall be cognizable and the offences punishable with imprisonment of three years shall be bailable. After the 2008 Amendment Act, Section 78 provides that the power to investigate the offence under this Act is with a Police Officer not below the rank of Inspector.

5.1.4. The Consumer Protection (E-Commerce) Rules, 2020

The Central Government, Ministry of Consumer Affairs, notified on July 23, 2020, the Consumer Protection (E-Commerce) Rules, 2020 (Rules) under the Consumer Protection Act, 2019 (Act), with an intent to prevent illegal trade practices in e-commerce and defend interests and rights of consumers. The new rules will also apply to e-commerce sites like Amazon, Flipkart, Snapdeal. It has several strict provisions for e-commerce sites. The seller of counterfeit and adulterated goods can be subject to life imprisonment.

5.1.4.1 Scope and Applicability of the Rules

The Rules will apply to (i) all goods and services bought or sold over digital or electronic networks, (ii) all models of e-commerce, and (iii) all formats of e-commerce retail, to the exception of natural persons transacting in their personal capacity (which is not part of any professional or commercial activity undertaken on a regular or systematic basis). In the absence of any guidance on what ‘regular or systematic basis’ means, a plain reading of this exclusion makes it very narrow.

The Rules govern electronic commerce entities (“platforms”), which own, operate or manage, a digital or electronic facility or platform for electronic commerce, and sellers of products and services.

E-commerce sites like Amazon, Flipkart will have to give all kinds of information to the consumer. Help the consumer decide shopping, inform the consumer about the details of the agreement entered into with the vendors, the address of such vendors, place of manufacturing the product along with the expiry date, payment gateway safety and customer care number. Under the new rules for settling disputes of consumers, no fee will be charged for filing a case up to five lakh rupees. Consumers have to explain the ways in which they can complain against a seller. They will also get updates on the process of hearing their complaint.

5.1.4.2 Obligations of Online Platforms

More importantly, the rules have been expressly applied to digital products and e-commerce entities which, although not established in India, “consistently” offer goods or services to consumers in India.

The most noticeable thing that the rules will apply to entities offering purely digital offerings such as over-the-top content provider platforms, ed-tech offerings, cab-hailing/ sharing companies, event management/ ticket vending platforms, telemarketing channels, etc., or B2B businesses (which may not have been covered earlier.[6]

5.1.4.3 Compliance Officer:

According to the new rules, it is an obligation on online platforms to appoint a nodal officer or a temporary senior functionary, who is an Indian resident, to ensure compliance with the act and the rules. No qualifications or duties (or liabilities) of such an officer have been prescribed. Additionally, what needs to be done to satisfy this requirement in substance also remains unclear.

5.1.4.4 Consumer Grievances

The new law gives consumers the option to file complaints electronically from anywhere. They can file a complaint with any consumer commission near their home. The rules regulate major requirements in relation to consumer complaints, including the establishment of a complaint redressal

[6]Consumer protection e-commerce rules need for more clarity, *available* at: https://corporate. cyrilamarchandblogs .com (last visited on June 08, 2021)

mechanism with specified deadlines, the appointment of a complaints officer and the establishment of a process allowing consumers to track their complaints. It is noted that the new rules are silent on the details of the adequacy of the complaint redressal mechanism. This may be an opportunity for industry bodies or self-regulatory organizations to formulate a set of standards to define the norm.

5.1.4.5 Duties and Obligations of Marketplace E-Commerce Entities:

The rules require that online platforms publish a significant amount of information in a clear and accessible manner. Information requirements vary for inventory-based platforms and marketplace platforms, the latter being required to publish information, including the country of origin of goods. The rules do not specify how this would be assessed, especially for assembled products, refurbished products, or products manufactured in one country, under license, by an entity in another country.[7]

In addition, the rules require marketplace e-commerce entities to ensure that sellers on their platform agree that information about products and services directly matches the general characteristics of those products or services. Marketplace e-commerce entities are also required to post, inter alia, the terms and conditions generally governing their relationship with sellers on its platform, including a description of any differential treatment; payment methods and details (including the address and contact details) of sellers.

Marketplace e-commerce entities cannot claim immunity under the safe harbor provision of Section 79(1) of the Information Technology Act 2000 with regards to any liability for the information of third parties, made available on its platform, unless they observe due diligence when providing such information to consumers on their platforms in accordance with Section 79(2) and (3) of the IT Act.

[7] Consumer protection e-commerce rules need for more clarity *available* at : http://cam.a2zportals.co.in (last visited on June 08, 2021)

5.1.4.6 Duties and Obligations of Sellers on Marketplace E-Commerce Platforms and Inventory E-Commerce Entities:

The new rules clearly restrict the online sellers on marketplace e-commerce entities and the inventory e-commerce entities from using any unfair trade practice, posting false reviews, representing itself as a consumer, any advertisement relating to goods or services that represent a fallacious or fake picture. Moreover, such e-commerce entities cannot deny to take goods back or discontinue the services purchased or agreed to be purchased, if such goods or services were defective or delivered late. Furthermore, as the “inventory e-commerce entities” are direct sellers their compliance requirements are on similar lines to those applicable to the sellers on “marketplace e-commerce entities”.[8]

5.1.4.7 Pricing, Purchases, Refunds and Cancellations:

The platforms are subject to a widely formulated restriction against the manipulation of the prices of goods or services offered to them, in order to make an unreasonable profit by imposing any unjustified price on consumers. Although the rules prescribe criteria such as existing market conditions, the nature of the goods or services and extraordinary circumstances to assess whether the price is unjustified. In the absence of clear parameters, this restriction will result in the implementation of well-known practices, ranging from pricing to preferred customer privileges and selective discounts.

No cancellation fees can be imposed unless a similar fee is payable by the platform entity for cancellation. This can impact particularly those business models wherein the paid charges after cancellation of order cannot recover the cost of such an order. For example, a platform focused on grocery shopping or a food delivery service, having an order cancelled after perishable goods are dispatched for delivery, would be unable to recover costs and might also be unable to penalise irresponsible behavior of consumers

[8] E-commerce rules2020, *available at* https://www.mondaq.com (last visited on June 08, 2021)

If an inventory-based platform expressly or implicitly guarantees the authenticity of the goods/services sold by it, or guarantees that such products/services are genuine, or anything else pertaining to the authenticity of such products/services, then it has to take proper responsibility in that regard. Terms and conditions will need to be developed to clarify what is approved by the platform.

However, the question remains that will such e-commerce websites now be able to hide anything from consumers?

The Consumer Protection (E-Commerce) Rules 2020 provide for an exhaustive mechanism to deal with aspects of returns, refunds and associated processes, which have been made easier for the online retailer while keeping in mind the best interest of consumer. The e-commerce rules will apply to all e-retailers who are offering products and services to Indian consumers, then, whether their registered office is in India or abroad.

It has exhaustively provided for additional responsibilities which will now apply on all e-commerce sites such as Amazon, Flipkart, e-bay, etc. which will be required to facilitate all kinds of necessary information to their consumers. This will also ensure greater transparency and awareness creation amongst consumers. It will ensure that there is no discrimination against customers or against vendors.

Consumers will be made aware of the ways in which they can file a complaint against a seller. They will also get updates on the process of hearing their complaint. Till now vendors used to be responsible, but now e-commerce companies will also be responsible, since, the product featured on their platform has been purchased by paying at their gateway.

The rules provide for strict disclosure and compliance requirements and strict penalties in case of non-compliance. Given that the rules are in effect from the date of its notification and do not consider a window of compliance, it would be interesting to assess how e-commerce entities will comply and how government will enforce these rules. It will further be interesting to see the implementation and application of the said rules on account of the present day geopolitical clash between India and China.

5.1.4.8 Highlights of the New Law and the New Rules

- Last year, the Parliament approved the Consumer Protection Bill 2019. This new law will replace the Consumer Protection Act 1986. The new law came into effect from 20th July 2020.
- Though this law was enacted in August last year, however, on account of the uncertainty pertaining the rules, it could not be applied.
- Under the new legal framework accountability of e-commerce is key. Accountability of e-commerce, online, direct selling and teleshopping companies has been fixed.
- At present, no decision has been taken by the Central Government regarding the enforceability of sections 10 to 27 of the Consumer Protection Act 2019.
- The period for appealing from the decisions of the District Commission to the State Commission have been increased from 30 to 45 days. Furthermore, the district, state and national commissions would have the power to review their decisions.
- An e-commerce consumer has been defined as a consumer under the new law.
- Now PIL can also be filed before the consumer forum.

i) Pecuniary Jurisdiction

- The central government has made several changes in this law. Till now, the District Consumer Forum used to hear cases up to Rs 20 lakh. It has been increased to one crore rupees.
- At present, the consumer had to file a petition in the State Commission on complaints of more than 20 lakhs. According to the

new law, cases above one crore rupees and up to 10 crore rupees will be able to go before the State Commission.

- Cases of more than Rs 10 crore will go to the National Commission.

ii) Freedom to complain from anywhere:

- The new law gives consumers the option to file complaints electronically from anywhere. They can file a complaint with any consumer commission near their home.
- Earlier they had to complain where they bought the goods or where the seller's registered office was located, however this requirement no longer exists.
- Under the new rules for settling disputes of consumers, no fee will be charged for filing a case up to five lakh rupees.
- According to the new law, if the complainant is unable to participate in the hearing of the case in person, he can be participate through through video conferencing.

iii) Provision of life imprisonment in the event of death by counterfeit goods:

- Consumers can bring manufacturers and vendors to court for adulteration and counterfeit goods and thereafter seek damages.
- Under the new law, the manufacturer and seller will be responsible for compensating for the injury or damage caused by the defective product or service.
- If there is no injury to the consumer due to the defective product, the seller may face a fine of up to 6 months and a fine of up to one lakh rupees.
- If the consumer gets hurt due to the defective product, then the maximum jail sentence for the seller of goods will be 7 years and the fine will also increase to five lakh rupees.

- If a consumer dies due to a defective product or service, the seller will be punished with imprisonment for seven years. The fine will also be 10 lakh rupees.

iv) Accountability of celebrity advertisers also fixed

- Celebrities can also be fined up to Rs 10 lakh for misleading advertisements. It will be the responsibility of the celebrity to investigate the claim made in the advertisement.
- There is a provision for penalty and compensation on companies for adulterated goods and bad products. A false complaint will now attract a fine of up to 50 thousand rupees.

v) Central Consumer Protection Council to be formed with 35 members

- Under the Consumer Protection Act 2019, the Central Consumer Protection Council will be established as an advisory body on consumer related issues.
- The Council will be chaired by the Union Minister of Consumer Affairs and the Deputy Chairman of the Council shall be the Minister of State. Furthermore, there shall be 34 other members from different regions of the country.
- The Council will have a three-year tenure.
- It will have consumer affairs ministers from two states of each region i.e. North, South, East, West and North-East.

5.2 Content Regulation

Content regulations and compliance are extremely important for e-commerce enterprises as these enterprises distribute content or act as a platform for distribution or exchange of third party data/content. Section 79 of the rules made under the IT (Amendment) Act 2008, provides that intermediaries must observe due diligence to oversee appropriateness of all the contents. Besides, the "intermediaries" of information are required to adhere to different obligations and commitments and ensure due diligence while managing data of the third party and in effect data that intermediaries themselves choose to publish.

5.2.1 Indian Penal Code

Indian Penal Code was amended by introducing the expression "electronic". In this way, all the electronic documents and records were made comparable with the physical archives and records secured within the ambit of the Indian Penal Code. Further, the offenses were made culpable under IPC:

i) Section 292: Obscenity and Indecent Advertisement[9]

Section 292 describes the term obscene and provides for punishment for distributing any such object. Section 292 (1) defines the term obscene as follows:

"a book, pamphlet, paper, writing, drawing, painting, representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely having regard to all relevant circumstances to read, see or hear the matter contained or embodied in it." Further subsection (2) provides for the penal consequence in the following manner.

> "shall be punished on first conviction with imprisonment of either description for a term which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees".

Furthermore, if anything is committed by electronic means such as a computer, e-mail or any other digital medium, it shall also be treated as cyber

[9] Indian Penal Code, (Act 45 of 1860), s. 292

obscenity and shall be punishable under IPC section 292. Generally, the obscene material on the net would not fall under the ambit of section 292. But when section 292 is read with section 29(A) of the IT Act, it can be easily assumed that any digital medium can be constructed to be a document within the meaning of Section 29. It follows that if any explicit material, which is indecent, on the off chance that unmistakable on the PC screen, at that point an offense under area 292 of the I.P.C., is committed.

ii) Section 292 A:

Printing etc. of grossly indecent or scurrilous matter or matter intended to blackmail is punishable under this section.

iii) Section 354 C: Voyeurism

According to section 354 C voyeurism is**:**

"Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine".[10]

If any person who watches, or takes the picture of a woman engaging in a private act in circumstances where she would usually expect not to be observed, and the person circulates such images of a woman on the online platform, shall be punishable under this section.

iv) Section 354 D: Cyber Stalking

[10] Indian Penal Code, (Act 45 of 1860), s. 354C

As per the definition of section 354 D, if any man who

- follows a woman to contact her or contacts her to foster any interaction, repeatedly, despite the clear intention of disinterest by such person, or
- monitors a women by the use of the internet, e-mail, or any other digital medium, commits the offence of stalking under this section.

v) Section 420: Bogus Websites, Cyber Frauds[11]

Section 420 provides that "whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine."

For instance, where the complainants had alleged in the *Ajay Mitra case* of cheating, the Court held that even if the allegation made in the complaint is accepted to be true and correct, the appellants still cannot be said to have committed any offence of cheating. Since the appellants were not in the picture at the time when the complainant alleged to have spent money in improving the bottling plant, neither any guilty intention can be attributed to them nor could it be possible for the appellant to have the intention on his part to deceive the complainant.[12]

The offence of cheating is established when the accused thereby induces a person to deliver any property or to do or to omit to do something which he would otherwise not have done or omitted.[13]

[11] Indian Penal Code, (Act 45 of 1860), s. 420
[12] *Ajay Mitra v. State of Madhya Pradesh,* AIR 2003 SC 1069.
[13] *Mahadeo Prasad v. State of Bengal*, AIR 1954 SC 724.

vi) Sec. 463 IPC: E-mail Spoofing [14]

Email spoofing refers to a sender address that is forged to make it look as if it came from someone else. This is a common technique used by phishing attacks, spam, and malware to make their emails appear to be coming from legitimate sources, such as governmental authorities, insurance companies, and banks. They will frequently contain requests for confidential information, such as social security numbers or banking details, and requests to reset passwords.[15]

According to Section 463 of IPC:

"*Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.*"

vii) Sec. 464 IPC: Making a False Document

Section 464 provides provisions relating to false electronic record and any type of act under this section is punishable. Section 464 as follows:

A person is said to make a false document or false electronic record:

First, who dishonestly or fraudulently-

(a) Makes, signs, seals or executes a document or part of a document;

(b) Makes or transmits any electronic record or part of any electronic record;

(c) Affixes any digital signature on any electronic record;

(d) Makes any mark denoting the execution of a document or the authenticity of the digital signature, with the intention of causing it to be believed that such document or part of document, electronic record or digital

[14] Indian Penal Code, (Act 45 of 1860), s.463

[15] Security wordbook email spoofing, *available* at: https://www.avira.com (last visited on February 6,2020)

signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly, who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly, who, dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alterations.

viii) Sec. 468 IPC: Forgery for the Purpose of Cheating[16]

Whoever commits forgery, intending that the document or electronic record forged, shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

ix) Section 469 Forgery for the Purpose of Harming Reputation

As per section 469:

Whoever commits forgery, intending that the document or electronic record forged, shall harm the reputation of any party, or knowing that it is likely to use for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

[16] Indian Penal Code, (Act 45 of 1860), *s.468*

The purpose of this section is to punish hackers who make fake electronic records with the intention to harm the reputation and the goodwill of the others.

x) Section 499: Cyber Defamation

The term defamation is used to explain the injury that is caused to the reputation of a person in the eyes of a third person. The injury can be done by words spoken or written, or by signs or by visible representations. The intention of the person making the defamatory statement must be to lower the reputation of the person against whom the statement has been made in the eyes of the general public. Cyber defamation is a new concept but the traditional definition of the term defamation is applicable to cyber defamation as well since it includes the same ingredients of defamation, through a new and a digital medium.

The medium of cyber defamation may be as follows:

- World Wide Web
- Discussion groups
- Intranets
- Mailing lists and bulletin boards
- E-mail

The provision of section 499 is also applied in the matter of cyber defamation. According to section 499:

whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.[17]

[17] Indian Penal Code,(Act 45 of 1860), s.499

The act of defamation is punishable under Section 500 of IPC with simple imprisonment up to 2 years or fine or both.

5.2.2. Indian Evidence Act

In this segment, the researcher shall undertake a study of the relevant provisions pertaining to e-commerce under the Indian Evidence Act, 1872.

- Section 3 defines the term evidence and includes within its meaning electronic records as evidence.
- Section 17 defines the term admission as a statement, oral or documentary, or contained in electronic form which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons, and under the circumstances. Admissibility is substantive evidence of the fact admitted while a previous statement used to contradict a witness does not become substantive evidence and merely serves the purpose of throwing doubt on the veracity of the witness.[18]
- Section 22 provides for the circumstances in which an oral admission could be proved as to the contents of an electronic record. This section does not allow the evidence of oral admission as to the contents of an electronic record. It then talks of an exception, whereby, electronic records are presumed to be genuine but when the content of a document is in question, other evidence is liable to be taken. In such a case an oral statement may be taken in as evidence.
- According to Section 39[19] of the Evidence Act, when any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document,

[18] *Bishwanath Prasad v. Dwarka Prasad*, AIR 1974 SC 117.

[19] Indian Evidence Act, (Act 1 of1872), s.22A says, Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.

or is contained in a document which forms part of a book or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made. When evidence is given of a statement which forms part of (a) a longer statement, or (b) a conversation, or (c) an isolated document, or (d) a document contained in a book, or (e) series of letters of papers, or (f) electronic records, the Court has discretion as to how much evidence should be given of the statement, conversation, document, book, or series of letters or papers for the full understanding of the nature and effect of the statement and the circumstances under which it was made. The principle on which this section is based is that it would not be just to take part of a conversation, letter, etc., as evidence against a party without giving to the party at the same time the benefit of the entire residue of what he wrote or said on the same occasion. Thus, the rule enacted in this section will not warrant the reading of distinct entries in an account book, or distinct paragraphs in a newspaper, unconnected with the particular entry or paragraphs relied on by the opponent.[20]

- Section 47A[21] provides for the relevance of expert opinion in case of the genuineness of an electronic signature. According to this section when the court has to form an opinion as to the electronic signature of any person, the opinion of the

[20] Ratanlal & Dhirajlal, *The Law of Evidence*, 317 (21st Ed., Wadhwa & Co., Nagpur, 2009)

[21] Indian Evidence Act, (Act 10 of 1872), s. 47A says, when the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.

certifying authority which has issued the Electronic Signature Certificate is a relevant fact.

- Section 65A talks about the contents of electronic records which may be proved in accordance with the provisions of Section 65B. Section 65B prescribes the mode for proof of contents of electronic records. The primary purpose is to sanctify proof by secondary evidence. This provision of proof by secondary evidence would apply to any computer output, such output being deemed as a document. The section says in sub-section (1) that any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer and to be referred to as computer output, shall also be deemed to be a document. The section lays down particular conditions which have to be satisfied in relation to the information and the computer in question. Where those conditions are satisfied, the electronic record shall become admissible in any proceedings without further proof of the original as evidence of any contents of the original or of any fact affirmed in it.

- Section 67A talks about proof as to digital signature. It states that, except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such a digital signature is the digital signature of the subscriber must be proved.
- Section 73A[22] talks about the verification of digital

[22] Indian Evidence Act, (Act 10 of 1872), s. 73A says, in order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct—

that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

signatures. To determine whether a digital signature is that of the person by whom it purports to have been affixed, the court may direct that person or the controller or the certifying authority to produce the digital signature certificate. The court may also direct any other person to apply the public key listed in the digital signature certificate and verify the digital signature purported to have been affixed by that person.

- Section 85A provides that the court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

Section 85B provides that any proceeding involving a secure electronic record, the court has to presume, unless the contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

Sub-section (2) further provides that in any proceeding involving a secure digital signature, the court has to presume unless the contrary is shown, that the secure electronic signature was affixed by the subscriber with the intention of signing or approving the electronic record.

Sub-section (2) further provides that except in the case of a secure electronic record or a secure electronic signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature. A secure system is defined in Section 2(ze) of the IT Act.[23]

Section 85C also provides that a presumption is available to the

---

[23] Indian Evidence Act, (Act 10 of 1872), s. 47A s. 2 (ze) says, –secure system‖ means computer hardware, software, and procedure that— footnote continue on next page are reasonably secure from unauthorised access and misuse; provide a reasonable level of reliability and correct operation; are reasonably suited to performing the intended functions; and adhere to generally accepted security procedures.

court that, unless the contrary is proved, the information listed in an Electronic Signature Certificate is correct, except for information specified as subscriber information which has not been verified if the certificate was accepted by the subscriber.

Section 88A talks about the presumption of electronic messages. The section provides that the court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into the computer for transmission, but the Court shall not make any presumption as to the person by whom such message was sent.

Section 90A provides that where an electronic record purports to be or is proved to be five years old and is produced from any proper custody which the court considers proper in the particular case, the court may presume that the electronic signature which purports to be the electronic signature of any person was so affixed by him or by any person authorized by him in that behalf.[24]

5. 3. Consumer Protection Act, 2019[25]

The Parliament passed the Consumer Protection Bill, 2019 on 06.08.2019 to substitute the Consumer Protection Act, 1986 The President of India gave its assent to the Consumer Protection Act, 2019 on 09.08.2019 and the new law came into effect from 20th July 2020.The 2019 Act has been enacted for the purpose of presenting timely and effective administration and settlement of consumer issues and related matters.

The Central Government has not brought an amendment in Consumer Protection Act, 1986, instead of this, enacted a new Act altogether so as to provide enhanced protection to the consumers buying into consideration the

[24] Indian Evidence Act, (Act 10 of 1872), s.90A
[25] Consumer Protection Act, 2019, *available at* www.mondaq.com (last visited on February 26, 2020)

booming e-commerce industry and the modern methods of providing goods and services such as online sales, internet shopping, door to door selling and multi-level marketing in addition to the traditional methods of shopping.

The 2019 Act has brought in some major changes and provides for more protection to the consumers in *pari materia* to the earlier 1986 Act which can be seen from the comprehensive definition provided for the term 'consumer' and 'unfair trade practice'. The 2019 Act expands the scope of the definition of the term consumer to include the consumers involved in online transactions and also covers the customers engaging with e-commerce businesses within its ambit. The 2019 Act has also widened the definition of unfair trade practices as compared to the 1986 Act which now includes within its ambit misleading online advertisements, the practice of not issuing bills/memos for the goods and services; failing to take back defective goods or deactivate defective services and refund the amount within the stipulated time mentioned in the bill or memo or within 30 days in the absence of such stipulation, and disclosing personal information of a consumer unless such disclosure is in accordance with law.[26]

The 2019 Act has also introduced the concept of 'unfair contract' which includes those contracts, which favour the manufacturers or service providers and are against the interest of the consumers such as:

i) Contracts requiring manifestly excessive security deposits to be given by a consumer for the performance of contractual obligations;

ii) Imposing any penalty on the consumer for a breach of the contract, which is wholly disproportionate to the loss due to such breach to the other party to the contract;

iii) Refusing to accept early repayment of debts on payment of applicable penalty;

iv) Entitlement of a party to the contract to terminate such contract

[26] *Id.*at 25.

unilaterally, without reasonable cause;

v) Permitting or has the effect of permitting one party to assign the contract to the detriment of the other party who is a consumer, without his consent;

vi) Imposing on the consumer any unreasonable charge, obligation or condition which puts such a consumer to any disadvantage.

Such unfair consumer contracts are now covered under the 2019 Act and a complaint in this regard can now be filed by a consumer. This would help to keep a check on businesses including banks and e-commerce sites that take advantage of their dominance in the market and mandatorily require the helpless consumers to sign such unfair contracts and accept their standard terms before selling them goods or providing services.[27]

One of the most important additions to the 2019 Act is the proposal to establish the Central Consumer Protection Authority (CCPA), to regulate, protect and enforce the importance of the consumers and matters related to unfair trade practices. The new Act has been provided with broad powers to inquire, investigate and take action against violations of the new Act. Another important power the CCPA has been given is to take action and impose penalty against misleading and fake advertisement as well as against any endorser of such advertisement, which means the new Act now permits to take against even celebrities who have endorsed such misleading and false advertisement provided such celebrities failed to carry out any due diligence before engaging in such advertisements or promotion of any product.

In the Act, there is a provision of imposing a penalty of up to Rs.10 Lakhs for the first violation and up to Rs.50 Lakhs on every subsequent violation on a manufacturer or an endorser, for a false or misleading advertisement. In addition to this, such a company or endorser may be sentenced to imprisonment for up to two years. The Act has also been granted the authority to initiate suo-moto proceedings against violators, pass

[27] *Id.* at 26.

directions to recall products or suspend services and provide a refund to consumers and file class-action suits on behalf of various consumers which makes it an effective tool to curb mass violation of consumer interest.

Another significant presence in the 2019 Act is the idea of product liability which covers within its ambit the product manufacturer, service provider and seller, for any claim for compensation. The term ‘product liability’ is defined by the 2019 Act as the obligation of a product manufacturer or product seller, of any product or service, related to the product to compensate for any injury caused to a consumer by such defective product manufactured or sold or by insufficiency in services relating to the product. Additionally, since the product seller has now been determined to include a person who is involved in placing the product for a commercial purpose and as such would include e-commerce platforms as well. Accordingly, the ground commonly taken by e-commerce websites that they merely act as ‘platforms’ or ‘aggregators’ will now not be trustworthy before the court anymore. There are extended obligations pertaining to risks of manufacturers as compared to product service providers and product sellers, considering that under the 2019 Act, manufacturers will be liable in product liability litigation even where they successfully prove that they were not negligent or dishonest in making the express warranty of a product. However, certain exceptions have been given under the 2019 Act from liability claims, such as, that the product seller will not be liable where the product which has been misused, altered or modified.

5. 3.1. Some Important Definitions under the Act

i) **Consumer**

As per the Act, that person is called a consumer who avails the services and buys any goods and services for self-use. It is notable that if a person buys any good and avails any service for resale or commercial purpose, is not considered a consumer under the new Act. This definition includes all types of transactions for example online and offline. Section 2 (7) of the Act defines a consumer as below:

"Consumer" means any person who—

(i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment, when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose; or

(ii) hires or avails of any service for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such service other than the person who hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first mentioned person, but does not include a person who avails of such service for any commercial purpose.

Explanation.—For the purposes of this clause,—

(*a*) the expression "commercial purpose" does not include use by a person of goods bought and used by him exclusively for the purpose of earning his livelihood, by means of self-employment;

(*b*) the expressions "buys any goods" and "hires or avails any services" includes offline or online transactions through electronic means or by teleshopping or direct selling or multi-level marketing;

ii) Rights of Consumers

Section 2(9) includes six consumer rights including the right to:

a) To be protected against marketing of goods and services which are hazardous to life and property.

b) To have information of the quality, quantity, potency, purity, standard and price of goods or services.

c) To be assured of access to a variety of goods or services at competitive prices.

d) To be protected from unfair or restrictive trade practices.

e) The right to be heard and to be assured that consumer's interests will receive due consideration at appropriate forum.

f) The right to consumer awareness.

iii) E-commerce

As per section 2(16), e-commerce includes all activities pertaining to buying or selling the product and services or any digital products over the digital network. Section 2(16) as follows:

"E-commerce" means buying or selling of goods or services including digital products over digital or electronic network.

(iv) Misleading Advertisement

According to section 2(28) false advertisement is punishable. In relation to service and goods misleading advertisement means:

a) False description of such product or service; or
b) Give a false guarantee to, or is likely to mislead the consumers as to the nature, substance, quantity or quality of such product or service; or
c) Convey an express or implied representation which, if made by the manufacturer or seller or service provider, would constitute an unfair trade practice; or
d) Intentionally conceals important information

(v) Central Consumer Protection Authority

Under section 10 of the Act, it is the responsibility of the Central Government to set up a Central Consumer Protection Authority (CCPA) to promote, protect and enforce the rights of consumers. The CCPA regulates matters related to violation of consumer rights, unfair trade practices, and misleading advertisements. The CCPA will have an investigation wing, headed by a Director-General, which may conduct inquiry or investigation into such violations.

5. 3.2. Comparison of the 1986 Act with the 2019 Act

Provision	1986 Act	2019 Act
Ambit of law	All goods and services for consideration. Free and personal services are excluded.	All goods and services, including telecom and housing construction, and all modes of transactions (online, teleshopping, etc.) for consideration. Free and personal services are excluded.
Unfair trade practices	Includes six types of such practices, like false representation, misleading advertisements, etc.	Adds three types of practices to the list, namely: (i) failure to issue a bill or receipt; (ii) refusal to accept a good returned within 30 days; and (iii) disclosure of personal information given in confidence, unless required by law or in public interest. Contests/ lotteries may be notified as not falling under the ambit of unfair trade practices.
Product liability	No provision	Claim for product liability can be made against the manufacturer, service provider and seller. Compensation can be obtained by proving one of the several specified conditions in the Act.

Unfair contracts	No provision	Defined as contracts that cause a significant change in consumer rights. Lists six contract terms that may be held as unfair.
Central Protection Councils (CPCs)	CPCs promote and protect the rights of consumers. CPCs established at the district, state, and national level.	Makes CPCs advisory bodies for promotion and protection of consumer rights. Establishes CPCs at the district, state and national level.
Regulator	No provision	Establishes the Central Consumer Protection Authority (CCPA) to promote, protect, and enforce the rights of consumers as a class. CCPA may: (i) issue safety notices; (ii) pass orders to recall goods, prevent unfair practices, and reimburse purchase price paid; and (iii) impose penalties for false and misleading advertisements.
The pecuniary jurisdiction of Commissions	District: Up to Rs 20 lakh. State: Between Rs 20 lakh and up to Rs 1 crore. National: Above Rs 1 crore.	District: Up to Rs 1 crore. State: Between Rs 1 crore and up to Rs 10 crore. National: Above Rs 10 crore.
Composition of Commissions	District: Headed by current or former District Judge and two members. State: Headed by a current or former High	District: Headed by a President and at least two members. State: Headed by a President and at least four members.

	Court Judge and at least two members. National: Headed by a current or former Supreme Court Judge and at least four members.	National: Headed by a President and at least four members.
Appointment	Selection Committee (comprising a judicial member and other officials) will recommend members on the Commissions.	No provision for Selection Committee. The Central Government will appoint through notification.
Alternate dispute redressal mechanism	No provision	Mediation cells will be attached to the District, State, and National Commissions.
Penalties	If a person does not comply with orders of the Commissions, such a person may face imprisonment between one month to three years or fine between Rs 2,000 to Rs 10,000, or both.	If a person does not comply with orders of the Commissions, he may face imprisonment up to three years, or a fine not less than Rs 25,000 extendable to Rs 1 lakh, or both.
E-commerce	No provision	Defines direct selling, e-commerce and electronic service provider. The Central Government may prescribe rules for preventing unfair trade practices in e-commerce and direct selling.

5. 3.2 Analysis of Consumer Protection Act, 2019

- The new Act sets up the Consumer Disputes Redressal Commissions as quasi-judicial bodies to adjudicate disputes. The new Act empowers the Central government to appoint members to these Commissions. The new Act does not specify that the Commissions will comprise a judicial member. If the Commissions were to have members only from the executive, the principal of separation of powers may be violated.
- Under the new Act, the Central government has power to appoint, remove and prescribe conditions of service for members of the District, State and National Consumer Disputes Redressal Commissions. The new Act leaves the composition of the Commissions to the Central government. This could affect the independence of these quasi-judicial bodies.
- Consumer Protection Councils will be set up at the district, state, and national level, as advisory bodies. The state and national councils are headed by Ministers in-charge of Consumer Affairs. The new Act does not specify who the Councils will advise. If the Councils advise the government, it is not clear in what capacity will such advice be given.
- Moreover, in India various sectors have their own law and regulations, duplication or conflicts between CCPA and these bodies may arise.;
- At this point, it is not clear in Act on whether matters currently pending before the Consumer Commissions will continue or if they are likely to get transferred on account of the change in pecuniary jurisdiction. This uncertainty will additionally add to delays. Already there are a large number of cases pending in district and state forums.
- While a commendable action, it is not clear as to how the Authority will essentially function, particularly since existing District Collectors have been given the task to undertake certain functions concerning inquiries and investigations. There is also an important overlap between the investigative wing and the search and seizure functions of

the District Collector, which are probably to lead to a potential clash of interest.

- As per the newly enacted consumer protection law, the second-hand C2B consumer is not considered as a consumer. The law does not protect such consumers who have sold a used product, while other forms of C2B e-commerce companies getting revenue from consumers are covered. It is important to note that this model of e-commerce is growing rapidly in the present e-commerce scenario. In spite of this, there is no clear law or policy for protecting such a consumer. If an e-commerce company cheats the consumer or lowers the price of goods based on immoral and harsh conditions. For instance, if the consumer wishes to return the product, he will have to wait for the company to send an agent for pick-up. However, if no agent came to pick up the product for a month, the company would subsequently inform that it is unable to do the same on account of unforeseen circumstances and would apologise for the inconvenience and ask the consumer to cancel the old order and place an order for a new one. Unfortunately, the new product will come at a reduced price by the company, however the consumer will nevertheless be compelled to make the subsequent purchase as he has no other option since the new act does not protect such a person as a consumer.

Indeed, several laws intended to protect consumers against such unlawful trade practices, false and misleading advertisements, nevertheless such unlawful practices continue to exploit consumers at an alarming rate. However, the new Act is laudable for its efforts to move further towards caveat venditor from the days of caveat emptor.

5.4. Judicial Response on E-commerce

In India, judiciary occupies one of the most important places in India’s democracy as one of its main pillars. It is the judiciary which interprets the law and its implementation and has the power to declare such a law *ultra vires* in case it violates the Constitutional provisions. Law relating to e-commerce in the new digital era is more or less techno-legal in nature. The Indian judicial system works under a settled legal environment, however there still remains several legal uncertainties, lacunas and technicalities pertaining to e-commerce. Therefore, the courts require assistance from experts on all technical issues pertaining to e-commerce related issues. In this regard section 45 of The Indian Evidence Act talks about expert opinion. It states as follows:

"When the Court has to form an opinion upon a point of foreign law, or of science, or art, or as to identity of handwriting or finger impressions, the opinions upon that point of persons especially skilled in such foreign law, science or art, or in questions as to identity of handwriting or finger impressions are relevant facts. Such persons are called experts."

Hence, courts can positively take expert opinion from a person who is well versed in computers and the internet and the court are not bound by expert opinion. Even if courts take any opinion from expert still it needs to arrive at its own autonomous conclusion. This sort of situation would cause some difficulties in the adjudicating process.

Order XIII of Code of Civil Procedure, 1908 needs marking of documents. In e-contract there are no primary documents and according to the Evidence Act, one needs to submit primary document. Courts in India decide practically all civil cases based on primary archives and as there are no primary documents in e-commerce, it is a bit hard for courts to handle cases pertaining to e-commerce.

In spite of the fact that substantive legal provisions in the form of the IT Act, 2002 have been put in place, nevertheless there is a dire need to provide similar procedural law pertaining to techno-legal issues which in turn compliments and supports the existing substantive law. IT Act is a substantive law that deals rights and liabilities of parties, though no such law is authorized in order to deal with the procedure. By not establishing procedural law for IT Act, the lawmakers have created an obstacle in its proper implementation, including its application by the judiciary. Therefore, the lack of proper procedural laws has created a substantial hurdle for the judicial system to determine matters pertaining to e-commerce.

5.4.1. Case Law Relating to E-Commerce

i) Amway India Enterprises Pvt. Ltd. v. *1Mg Technologies Pvt. Ltd. & Anr*., CS(OS) 410/2018.

The Delhi High Court has restrained e-commerce platforms Amazon, Flipkart, Healthkart and Snapdeal and several sellers from displaying, advertising and offering for sale the products of companies that are 'direct selling entities' without their consent. The interim injunction was passed on July 9th by a Single Judge Bench, in clubbing of suits filed by direct selling entities like Amway, Modicare and Oriflame which deal in healthcare and beauty products. The companies alleged that the aforementioned e-commerce platforms are sourcing and selling their products in an unauthorized manner at cheaper rates, resulting in financial losses to companies.

The Court observed that the companies have established their case against e-commerce platforms on the following grounds that:

- Direct Selling Guidelines have the force of law**:**

The Court held that the Guidelines have been issued by a gazette notification, therefore they constitute binding executive instructions. Therefore, both sellers and the e-commerce platforms are required to take the consent of the Direct Selling Entities before selling such products, as required by Clause 7(6) of the Guidelines.

Also, the Court opined that the "while the Defendants' (e-commerce platforms) and sellers insist on their Article 19(1)(g) rights being jeopardised, what it has lost sight is the fact that the Plaintiffs' (the companies) right to carry on business is being affected on this account. Further, the rights of genuine consumers are being affected, as is evident from the various comments, which consumers have put up on these platforms, after purchasing the Plaintiffs' products from the said platforms".

- The unauthorized sale of products on e-commerce platforms constitutes passing off, misrepresentation and dilution/tarnishment of their mark**:**

The Court observed that in order to use the companies trademark for displaying, advertising and offering for sale the disputed products, the products are required to be genuine. However, the Court relied on the reports of the Local Commissioners who inspected the premises of certain e-commerce platforms and noted that "there is a large scale of tampering of goods that is taking place".

As the platforms are facilitating the sale of the tampered products while hiding the sellers' contact details and portraying it as the companies' genuine product without their consent, such unauthorized sale constitutes passing off, misrepresentation and dilution/tarnishment of the companies' marks, products and businesses.

- The e-commerce platforms do not come within the ambit of the safe harbour protection:

For the intermediaries that are seeking exemption from liability, it is required of them to satisfy conditions contained in Section 79(2) of the Information Technology Act. As per Section 79(2) (c) of the IT Act, due diligence would have to be observed by the intermediaries in terms of setting up proper policies for IPR protection and for taking down of objectionable content. Further, it was held in the case of *Shreya Singhal v. Union of India*[28] that in order to be an intermediary, an online platform has to comply with due diligence requirement as per the platforms' own policies and as per the Intermediary Guidelines, 2011.

The Court held that as the defendants have failed to fulfil the requirement of due diligence as per their platforms' own policies and therefore they are not entitled to intermediary protection under Section 79.

- E-commerce platforms guilty of wrongful interference with the contractual relationship of the companies with their distributors/direct sellers:

The Court held that the platforms "are not merely passive non-interfering platforms, but provide a large number of value-added services to the consumers and users". Upon being notified by the companies of unauthorised sales on their platforms, they have a duty to ensure that the contractual relationships between the companies and their distributors/ direct sellers are not unnecessarily interfered with by their businesses. Conclusively, the court observed that the balance of convenience is in favour of the companies. The Court said that "irreparable injury would be caused to plaintiffs, their businesses, and all those who depend on plaintiffs' successful business, such as employees, distributors/direct sellers, agents, and finally the consumers if interim relief is not granted".

5.4.2. Case Law on Cyber Crime[29]

i) *Fatima Riswana v. State Rep. by ACP., Chennai & Others,* AIR 2005 SC 712.[30]

---

[28] AIR 2015 SC 1523.
[29] Case Law on Cyber Crime, *available at* www.cyberconsulting.com (last visited on February 26, 2019)
[30] *Fatima Riswana v. State Rep. by ACP., Chennai & Ors,* AIR 2005 SC 712.

The accused was facing trial for offences punishable under Section 67 of Information Technology Act, 2000 r/w Section 6 of Indecent Representation of Women (prohibition) Act, 1986, under Section 5 & 6 of Immoral Traffic (Prevention) Act, 1956, under Section 27 of Arms Act, 1959 And Sections 120(B), 506(ii), 366, 306 & 376 I.P.C. The appellant was a prosecution witness in S.C. No. 9 of 2004 wherein respondents 2 to 6 were the accused facing trail for offences punishable under the said provisions. The said trial was related to the exploitation of certain men and women by one of the accused Dr. L. Prakash for the purpose of making pornographic photos and videos in various acts of sexual intercourse and thereafter selling them to foreign websites.

The session's trial came to be allotted to the Fast Track Court V, Chennai which is presided over by a lay Judge. When the said trial before the Fast Track Court V was pending certain criminal revision petitions came to be filed by the accused against the orders made by the said court rejecting their applications for supply of copies of 74 Compact Discs (CDs) containing pornographic material on which the prosecution was relying. The said revision petitions were rejected by the Madras High Court by its order dated 13th February, 2004 holding that giving all the copies of the concerned CDs might give room for copying such illegal material and illegal circulation of the same. However, the court permitted the accused persons to peruse the CDs of their choice in the Chamber of the Judge in the presence of the accused, their advocates, the expert, the public prosecutor and the Investigating Office and also observed that the case be transferred to another court with competent jurisdiction presided by a male officer at the option of the sessions judge. Taking the same into account, the accused filed a revision petition for transferred to Fast Track Court IV which was presided by a male officer and the appellant alleged that she would be embarrassed if the trial is conducted by the male presiding officer. Moreover, the appellant stated that the Lady sessions judge didn't object to the trial of the case in the Fast Track Court V and the high court has erred in transferring the case and the Appellant was not given any opportunity of being heard before the alleged transfer. The learned counsel for the respondents contended that the appellant, though arrayed as a witness, was for all-purpose an accused herself and the law officer appearing in the case had expressed their embarrassment in conducting the trial before a lady Presiding Officer and even though the Presiding Officer did not expressly record her embarrassment, it was apparent that she too wanted the case to be transferred to another court, therefore, this Court should not interfere with the order of transfer. It was held that this appeal has to be allowed and the trial be transferred back to the Fast Track Court V, Chennai.

ii) *Avnish Bajaj v State (N.C.T.) of Delhi ,(*2005) 3 Comp LJ 364 (Del).[31]

The accused is the CEO of Baaze.com, an e-commerce company which facilitates the sale of any property, for which it receives commission and also generates revenue from advertisement carried on its web page. In the present case, counsel for the State argued that the accused was remiss, at the pain of culpability, in not stopping payment through banking channels after learning of the illegal nature of the transaction. It was strenuously contended that if bail was not granted it would adversely impact e-commerce, for which India may be the eventual loser. However, ultimately these considerations would not effect the decision of the Court whether to grant the bail or to reject it.

Mr. Jaitely, counsel for the petitioner, underscored that in Section 67 of the Information Technology Act, 2000 is an offence committed by a person who publishes or transmits any material which is lascivious or appeals to the prurient. Sections 292 and 294 of the Indian Penal Code were also mentioned which contemplate the selling, letting on hire, distribution or public exhibition or in any manner puts such material in circulation. He thus emphasized that the provision does not bring within its sweep the causing of the transmission in contradistinction to the publication of obscene material. Prima facie it

[31] *Avnish Bajaj v State (N.C.T.) of Delhi ,(*2005) 3 Comp LJ 364 (Del).

wasn’t established from the evidence gathered that any publication took place by the accused, directly or indirectly and that the actual obscene recording/clip could not be viewed on the portal of Bazze.com.

It was held that the accused actively participated in the investigations, and nothing was even argued before it in contrary by counsel for the State. The nature of the alleged offence was such that the evidence had already been crystallised and maybe was even tamper proof. Even though the accused is no longer an Indian National, he was of Indian origin with family roots in India. It cannot possibly be argued that a foreign national is disentitled to the grant of bail. The accused was released on bail subject to furnishing two sureties of Rs. 1,00,000/- each to the satisfaction of the concerned Court/ Metropolitan Magistrate/Duty Magistrate. Furthermore, the accused was not to leave the territory of India without the leave of the Court and for this purpose shall surrender his passport to the Magistrate. It was implicit in the grant of bail that he shall participate and assist in the investigation. The bail application was accordingly disposed of.

This matter relates to an internet website scandal where on an internet website carried the video clip shot on a mobile phone of two children of a school in Delhi indulging in an explicitly sexual act was listed for sale.

The website baaze.com provided an online platform or market where a seller and a buyer could interact. The petitioner, who was the Managing Director (MD) of the company that owned the website at the relevant point in time, asked the Court to annul the criminal prosecution for the offences of making available for sale and causing to be published an obscene product, which was the abovementioned clip, within the meaning of Section 292 Indian Penal Code (IPC) and Section 67 of the Information Technology Act 2000. The petition was filed under Section 482 of the Code of Criminal Procedure 1973 (CrPC) and raised questions concerning the criminal liability of directors for the offences attributable to a company, both under the IPC as well as the IT Act, particularly when such company was not arraigned as an accused.

The Court held that as far as IPC was concerned, there was no automatic criminal liability of a director where the company was arraigned as an accused. The absence of such a provision in the IPC could be viewed as a lacuna but it must not be presumed lightly as there were numerous statutes enacted by Parliament thereafter which have incorporated provisions to that effect. For instance, Section 85 of the IT Act was similarly worded as Section 141 NI Act and incorporates a deemed criminal liability of the director. The IT Act amends certain provisions of the IPC as well. But Parliament has chosen not to make any amendment to incorporate such a provision in the IPC. The Court has therefore to proceed with the law as it exists, particularly since it is a penal statute which admits strict construction.

The Court held that the case against the petitioner of the offence under Sections 292 and 294 IPC would be quashed and the proceedings with regards to Section 85 IT Act would continue.

iii) *Syed Asifuddin and Ors. v. The State of Andhra Pradesh and Anr.*, 2005 Cri LJ 4314.[32]

These two petitions were filed by different persons under section 482 of the Code of Criminal Procedure, 1973 seeking similar relief. Both the matters were admitted on the same day and since then both the matters were disposed of by a common. The petitioners in both the matters sought the relief of quashing FIR No. 20 of 2003 of Criminal Investigation Department (CID) Police, Hyderabad, registered under section 409, 420 and 120B of Indian Penal Code, 1860, Section 65 of the Information Technology Act, 2000 and Section 63 of the Copyright Act, 1957.

[32] *Syed Asifuddin and Others. v. The State of Andhra Pradesh and Anr.*, 2005 Cri LJ 4314

While admitting the petition, the Hon’ble Court passed orders in criminal Miscellaneous Petition No. 3951 of 2003 staying all further proceeding including investigation pending for the disposal of the main petition. The Public Prosecutor filed criminal miscellaneous petition No. 232 of 2005 for vacating the said order. The matter was finally heard at that stage and was disposed of finally. The main allegation against the petitioners was that the Mobile Identification Number (MIN) of Reliance phone was irreversibly integrated with the Electronic Serial Number (ESN) and the petitioners hacked ESN so as to wean away Reliance India Mobile (RIM) customer to TATA Indicom service. The question was whether the manipulation of this electronic 32-bit number ESN programmed into Samsung N191 and LG-2030 cell phone instruments exclusively franchised to second respondent amounted to altering source code used by these computer handsets i.e., cell phone instruments. In the background facts, a question would also arise whether such alteration amounts to hacking with computer system? If the query was answered in the affirmative, it is always open to the police to alter the FIR or it was always open to the criminal Court to frame a charge specifically with regard to hacking with the computer system, which was an offence under Section 66 of the IT Act. At this stage, it is pertinent to read Sections 65 and 66 of the IT Act.

Crime No. 20 of 2003 in so far as it was under section 409, 420 and 120B of Indian Penal Code, it was quashed and insofar as the crimes under Section 63 of the Copyright Act, 1957, the criminal petitions were dismissed. The CID Police, which registered Crime No. 20 of 2003, was directed to complete investigation and file a final report before the Metropolitan Magistrate competent to take cognizance of the case within a period of three months from the date of receipt of this order. The criminal petitions were accordingly dismissed.

iv) *D'zine Garage Pvt. Ltd. rep. by its Director Mr. Hari Sethuraman; D'zine Café FZE & D'zine Café FZE v D'zine Garage Pvt. Ltd. rep. by its Director Mr. Hari Sethuraman,* 2008 (36) PTC 614 (Mad).[33]

Plaintiff registered proprietor of the service mark 'D'zine' filed suit for permanent injunction against applicant-defendant who was using the mark 'D'zine' café as a service mark and as part of their corporate name and domain name 'www.Dzinecafe.com'. The respondent/plaintiff contended that the applicant-defendant deliberately adopted a similar service mark/trade name i.e. 'D'zine' café in a calculated attempt to cash in on the reputation and goodwill enjoyed by the respondent/plaintiff and to get illicit and quick gains without putting any substantial efforts. An interim injunction was therefore granted and hence, application was filed by the defendant to vacate the interim injunction and to reject the plaint. The applicant-defendant contended that the respondent-plaintiff had no office in India and hence the present Court has no jurisdiction to try the matter and therefore, the plaint was liable to be rejected. Ultimately, the Court held that in order to justify an order of rejection of plaint, the defendant would be required to show a very strong case in his favour and the power would be exercised sparingly and only in exceptional cases, since it would interfere with the right of the party to proceed with the trial. Since the defendant was unable to make a case, it was held that application for rejection of plaint was not maintainable.

Thereafter, the defendant sought vacation of interim injunction on the ground that the registration is for a logo only and that 'D'zine' was not a coined word, it is a corrupt from of design and was commonly in use. It was further contented that, 'D'zine' café was sufficiently different and not likely to mislead others and was also being used by many other. Held, for granting interim injunction phonetic similarity could not be ignored and the prior user must be proved and the subsequent use by the accused must indicate dishonest intention in its use. In the instant case, there was phonetic similarity and

[33] *D'zine Garage Pvt. Ltd. rep. by its Director Mr. Hari Sethuraman; D'zine Café FZE & D'zine Café FZE. by its Director Mr. Hari Sethuraman*, 2008 (36) PTC 614 (Mad).

moreover, the word 'D'zine' was not a generic word, it cannot be said to carry distinctive reference to a particular trade, becoming publici jiris. Since the business of the parties was almost the same and the fact that one was 'D'zine' café and the other was 'Dzine' garage, clientele was likely to be confused and would assume the two to be the same. In this case, the Plaintiff was held as the prior user. Furthermore, there was no specific denial of the charge that the defendant was taking advantage of the plaintiff mark. Usage of the same word by others and the argument that the word was a common word was held not to be a proper defence in an action for interim injunction. Thus, interim injunction was granted.

v) *Nirav Navinbhai Shah & Ors. v State of Gujarat and Anr.*, 2006 SCC Online Guj 174.[34]

The applicants, original accused in crime I.C.R. No. 54 of 2004 dated 26.02.2004 registered with Sector 7 police station Gandhinagar for offences punishable under Sections 381, 408, 415, 418, 420 read with Sections 34 and 120B of the Indian Penal Code and Section 66 and 72 of the Information Technology Act, 2000 preferred an application under Section 482 of the Code of Criminal Procedure 1973 for quashing of the said FIR and the resultant Criminal Case No. 3528 of 2004 before the Judicial Magistrate First Class Gandhinagar. The was mainly based on the grounds that the facts and allegations leading to lodging FIR pertained to a civil dispute and as the same had been amicably settled between the parties, no useful purpose would be served in continuing the criminal proceedings, rather continuation of same would be counter productive to the interest of justice.

Moreover, the complaint also does not contain any essential ingredient for maintaining criminal proceeding for the alleged offences. As it's stated in the arguments of the learned counsels that the parties have filed civil suits also in respect of the same dispute. The entire dispute between the parties was

[34] *Nirav Navinbhai Shah & Ors. v State of Gujarat and Anr.*, 2006 SCC Online Guj 174

resolved by amicable settlement. The alleged hacking was perpetrated on the complainants computer system only which said to have data pertaining to its client. The Counsels have submitted that on same of the web sites these data are already available. The dispute appears to be private in nature. The offence alleged is not strictly affecting or infringing any other individual or citizen. Thus, looking at the nature of the disputes, it could well be said that the continuation of the same was not in the interest of justice. It was held that the FIR 54 of 2004 registered at Sector 7 Police Station Gandhinagar and resultant Criminal Case No. 3528 of 2004 pending before the JMFC Gandhinagar were held to be quashed in the interest of justice.

vi) *Cyber Defamation Case: SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra*, Suit No. 1279/2001 Delhi HC. [35]

In India's first case relating to cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails and passed an important ex-parte injunction.

In this case, the defendant Jogesh Kwatra being an employee of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from indulging in such illegal acts of sending derogatory emails to the plaintiff.

On behalf of the plaintiffs, it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India

[35] *Cyber Defamation Case: SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra,* Suit No. 1279/2001 Delhi HC.

and the world. He further contended that the acts of the defendant in sending the emails had resulted in the invasion of the legal rights of the plaintiffs.

Further, the defendant was under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employee could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant. After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-parte ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs.

This order of the Delhi High Court assumes tremendous significance as this is for the first time that an Indian Court took up the jurisdiction in a matter concerning cyber defamation and granted an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

vii) Case Law *on Phishing: Nasscom v. Ajay Sood & Others*, 119 (2005) DLT 596.[36]

This was a landmark judgment in the case of the National Association of Software and Service Companies v. Ajay Sood & Others, delivered in March, 2005, wherein the Delhi High Court declared 'phishing' on the internet to be an illegal act, resulting in an injunction and recovery of damages.

[36] *Nasscom v. Ajay Sood & Others*, 119 (2005) DLT 596.

Elaborating on the concept of ‘phishing’, in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party’s advantage. The court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The Delhi High Court stated that even though there was no specific legislation in India to penalise phishing, it held phishing to be an illegal act by defining it under Indian law as “a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused”. The court held that the act of phishing also amounted to passing off and in effect tarnished the image of the plaintiff.

The plaintiff, in this case, was the National Association of Software and Service Companies (Nasscom), India’s premier software association. The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of head-hunting, the defendants composed and sent e-mails to third parties in the name of Nasscom.

The High Court recognised the trademark rights of the plaintiff and passed an ex-parte ad-interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associated or a part of Nasscom.

The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case.

Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered that the hard disks seized from the defendants' premises to be handed over to the plaintiff who would in turn be the owner of the said hard disks.

This case achieves clear milestones since it brings the act of "phishing" into the ambit of Indian laws even in the absence of specific legislations. It clears the misconception that there is no "damages culture" in India for violation of IP rights. This case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

viii) Case on Cyber Stalking: Manish Kathuria v. Ritu Kohli (C.C.No. 14616/2014)

Ritu Kohli Case, being India's first case of cyber stalking, was indeed an important revelation into the mind of the Indian cyber stalker. A young Indian girl being cyber stalked by a former colleague of her husband, Ritu Kohli's case took the imagination of India by storm. The case which got cracked however predated the passing of the Indian cyber laws and hence it was just registered as a minor offences under the Indian Penal Code.

ix) Arif Azim case

Arif Azim's case was India's first convicted cybercrime case. A case pertaining to the misuse of credit card numbers by a call center employee. This case generated a lot of interest. This was the first case in which a cybercriminal was convicted in India. However, keeping in mind the age of the accused and no past criminal record, Arif Azim, the accused was sentenced to probation for a period of one year.

x) The Arzika case

Pornography and obscene electronic content have continued to engage the attention of the Indian mind. Cases pertaining to online obscenity, although reported in the media, often are not registered. The Arzika case was the first in this regard.

5.5. Conclusion

This chapter was divided into two-parts; first part described law and policy relating to e-commerce and consumer protection and the second part of the chapter discussed some case laws relating to e-commerce and cybercrimes. All case laws were of the High Courts, since no case law decided by the Supreme Court of India in this regard was available.

Furthermore, though much advancement has been made at the international level but the legal developments in India pertaining to e commerce are still at the nascent stage. The Data Protection Bill 2019 and the Consumer Protection act, 2019 have been firm steps in the right direction. However the dilemma pertaining its implementation still persists. in the new CPA, 2019 Product warranty indicates the responsibility of the manufacturer, service provider or seller of the product. It is his responsibility to compensate the consumer for damages or damages caused by defects or services. To claim any compensation, the consumer must justify at least one of the conditions for defects or defects mentioned in the invoice.

In spite of the Consumer Protection Act, consumer awareness is the most important thing in e-commerce. However, the efforts to create awareness amongst consumers against cyber frauds and online cheating are not adequate in India because of a lack of digital literacy and proper infrastructure.

Law relating to e-commerce is a relatively new phenomenon and the nature of e-commerce regulation is techno-legal. The lack of technical environment of the judiciary has posed grave difficulties to keep up with the changing dimensions of technology and e-commerce issues and the cases arising thereof. At present, every nation has put in place their own legal framework and policy on e-commerce, thus there is always this question arising here as to which country's law would be applicable where the dispute pertains to an e-commerce transaction involving various countries. The researcher will discuss the critical jurisdictional issue pertaining to e-commerce in the next chapter.

CHAPTER-6

INTERNET JURISDICTION ISSUE AND E-COMMERCE

CHAPTER- 6

INTERNET JURISDICTION ISSUE AND E-COMMERCE

In the previous chapter, the author discussed the various aspects of legislations were analysed providing important insight into the procedural and substantive aspects of the existing legal framework in India related to e-commerce and cyber offences. Furthermore, it analyses the judicial approach pertaining to aspects of e-commerce cyber offences and the implementation of existing laws.

The present chapter describes in detail the legal provision on the issue of jurisdiction in e-commerce dispute. At the international level, legal provisions are very technical and not easy to understand since the present legal framework is more suitable for developed countries. Thus, the researcher also undertakes the study of Online Dispute Resolution system (ODR) as a possible solution to resolve the issue pertaining to jurisdiction issue. Furthermore, the ODR system provides for easy resolution of disputes as it is free of formalities and technicalities such as the rigours of procedure in the case of litigation and arbitration. The chapter is divided into two parts; first part deals with the relevant international laws on jurisdictional issues while the second part pertains to the Online Dispute Resolution system.

6. Introduction

E-commerce is an environment where there is no wall, no roof, no boundary; anyone can enter and go without hesitation and permission. When doing business and trading online, the restraints and limitations created on account of physical place, travel and transportation are no longer relevant and thus such restrictions may no longer be limiting on international trade where e-commerce services can take place, nothing will be difficult for sellers and buyers. Over the online format, consumer can order services and goods from different countries without a physical visit including consumers who can also buy personal goods abroad at home. The whole process of international trade and trade in general is made easier than ever by the fact that the number of transactions abroad has increased considerably. Due to the unrestricted nature of electronic commerce, electronic commerce matters are much more common and complex to handle than a paper transaction, since the location of electronic trading activity or the applicability of the law is very difficult to predict and to verify. Electronic commerce is not organized in a particular place and traders increasingly fear that electronic commerce is not enforceable in court because of legal obligations differing from country to country.

The word jurisdiction is based on the Latin "juris-dictio" which means "to say or speak the law". It demonstrates the value, validity and formulation of law.[1] The concept helps to define and determine power, the characteristics, property and conditions of the State under review within or outside the State. Generally, there are three types of jurisdiction, namely legislative, executive and judicial.

Jurisdiction to enact laws and enforcement of laws is the state's power to impose regulatory rules in this area.[2] However, the state must take into account the limitations of international law within its jurisdiction in cases involving non-regional entities. There is no concept of unlimited state jurisdiction because the state would not be willing to impose behavior that is not justified in practice. In reality, unlimited state authority seriously weakens the sovereign authority of another state. According to customary international rules, a state has no obligation to interfere in the internal and external affairs of another state in any manner or for any reason. Therefore, a state generally follows the principle of territoriality[3] or effect doctrine[4] its legislative power.

[1] Shunnagh Dorsett and Shaun McVeigh, Jurisprudence of Jurisdiction, 3 (1st edn., Oxon : Routledge - Cavendish, New York 2007) .

[2] Amit Sachdeva, *'International Jurisdiction in Cyberspace: A Comparative Perspective' available* at www.vaishlaw.com 2007(last visited on March 27,2020)

[3] See, Resolution Adopted by the General Assembly 2131 (XX) on Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty. ".No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of

The Indian Information Technology Act under sections 1 (2) and 75 of the Act includes the effects jurisdictional tests.

Jurisdiction to hearing a case or decide any dispute is the power and authority of a court. The court decides the jurisdiction of a matter on the basis of the subject matter, pecuniary value and local limits. The jurisdiction of a court generally depends on the regional nexus of the defendant and the cause of action. In the Indian context, the Code of Civil Procedure and Criminal Procedure Code incorporate the jurisdiction of the Court in the case of national and international aspects of issues.[5]

6.1 Characteristics of Internet Jurisdiction

The problem of appropriate jurisdiction always appears with the multinational character of e-commerce. Countries need to be able to ensure the equal protection of local businesses. Jurisdiction over e-commerce activities is specifically important in effecting this issue.

The clash between consumers and producers over jurisdictional issue is also relevant, since on the one hand, the sellers do not wish to be sued abroad whereas buyers always prefer to seek solutions within their own country. If there is no agreement on jurisdiction, then the lack of this equality means that e-commerce companies face the possibility of being subjected to any foreign legal jurisdiction in which their websites can be accessed. In practical terms, the most effective solution to resolve Internet private international law problems is to use ‘choice of jurisdiction’ and ‘choice of law’ clauses in electronic commerce as a means of agreeing to a common jurisdiction and choice of law, rather than leaving it to the inequality of geographically-oriented conflict-of-laws regime. However, most of the cases are not so straightforward. At present, there are no specific rules in the model laws and conventions

interference or attempted threats against the personality of the State or against its political, economic and cultural elements are condemned.”

4 Under Effect doctrine the State can provide jurisdiction over foreign conduct of outstate offender that produce the substantial effects within the territory

5 The jurisdiction of a court, *available* at https://epgp.inflibnet.ac.in (last visited on June 8, 2021)

dealing with Internet jurisdiction. The UNCITRAL Model Law on Electronic Commerce and the UN Convention on the Use of Electronic Communications in International Contracts (hereafter the UN Convention on Electronic Contracts) do not include any jurisdiction provisions, but the general provisions are important for analysing parties' location in internet transaction and are thus helpful for determining Internet jurisdiction and choice of law. The UN Convention on Electronic Contracts interprets relating facts i.e. the time and place of dispatch and receipt of data messages or electronic communication[6] and the location of the parties.[7] It directs to the location of the parties as well as to "the place of business", "the relationship to the relevant contract, the underlying transaction or the principal place of business", or "habitual residence".[8]

6.1.1 Difficulties in Determining Jurisdiction of Internet Cases[9]

The traditional notions of jurisdiction focus heavily on the location where the transaction in dispute took place in order to determine the proper jurisdiction and to adjudicate the dispute. However, internet transactions are conducted over a network, and as a result, it does not conform to traditional geographic boundaries. There are several ways that the infrastructure of the internet has made it difficult to establish the geographic location of the internet user, which are as follows:

(i) The internet is insensitive to geographic location and is designed to ignore rather than document geographic location.

(ii) Addresses on the internet are digital and not geographic addresses.

---

[6] UNCITRAL Model Law on Electronic Commerce, on the report of Sixth Committee (A/51/628) 16 December 1996, art.15 and UN Convention on the Use of Electronic Cornmunications in International Contracts,art.10 (hereafter UN Convention on Electronic contract)

[7] UN Convention on the Use of Electronic Communications in International Contracts ,2005, art. 6.

[8] Faye Fangfei Wang *"Internet Jurisdiction and Choice of Law: Legal Practices in The EU,US And China"* page 19 (Cambridge University Press 1st edition 2010)

[9] United States and European Union approaches to internet jurisdiction and their impact on e-commerce, *available* at www.upenn.edu/journales/volume25/issue1/chen25UPaJ. Int'lEcon.L.423(2004).pdf(last visited on March 01,2020)

(iii) The internet cannot feasibly be closed to users from another state as it is, by nature, an instrument of transnational commerce.

(iv) The user name and e-mail address are often the only indicators of a user's identity. As a result, a consumer buying goods through a web site may not be sure where the seller is located geographically.

(v) Information travels through many different paths through the internet which makes tracing difficult.

(vi) There is no way to avoid an internet user's message from reaching residents of any particular state

6.2. International Framework of Jurisdiction

To resolve the jurisdictional issues in online business, approximately all countries have put in place or the other laws, however such laws lack uniformity and thus create uncertainty and conflict. Here, the researcher has discussed some important laws which have gained international acceptance and recognition from countries like the United States, United Kingdom, European Union, etc.

6.2.1 Hague Convention 2005 on Choice of Court

The problem of choice of court agreement is important and significant in terms of the jurisdictional legal regime. At present, at the international level, the Hague Convention on Choice of Court Agreement 2005[10](hereafter pronounced "Choice of Court Convention") occupies a particularly important position. The Choice of Court Convention is a part of the draft of the Hague Convention on jurisdiction and international judgments in civil and commercial matters. The draft Jurisdiction Convention was considered to be an ambitious project. It was comprehensive but controversial, thus after a year of debating, the Hague Convention proposed that the Draft Jurisdiction Convention be

[10] Hague Convention on choice of court Agreement, concluded 30 june 2005, *Available at* www.hcch.net/index_enphp?act=covention.text&cid=98 cited by Faye Fangfei Wang *"Internet Jurisdiction and Choice of Law: Legal Practices in The EU,US And China"* 20 (Cambridge University Press 1st edition 2010)

scaled down to address only the issue pertaining choice of court agreements between businesses, leaving many of the broader jurisdictional and enforcement provisions on the cutting room floor.[11] On 30 June 2005, all of the Member States approved it as the Hague Convention on Choice of Court Agreements.[12]

The Choice of Court Convention has parallel functional similarity with the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards (1958) (New York Convention). The difference is in the characteristic forum between a The Choice of Court Agreement and an arbitration agreement. When parties choose a public forum, they will usually include a Choice of Court agreement. If the parties prefer a private forum, an arbitration agreement may be concluded. The Choice of Court Convention is a more modern and up-to-date international instrument than the New York treaty in the sense that the Choice of Court Convention recognises within its ambit the electronic choice of court agreement.

Can the approval of the Convention on Choice of Court address the issues raised in the following situations? To analyse these aspects it is pertinent to analyse this aspect through certain factual cases:

1. *A seller X is American and lives in London but X has a business company whose head office in Japan. A buyer Y is Spanish and lives in Dubai but Y establishes a factory in New York. Can X and Y choose the Rotterdam district court to hear their case when dispute arise?*

2. *If the buyer Y's company was established and situated in Paris instead and Y entered into a contract for sale of goods by automated electronic system while Y was travelling to the America, which court is competent to hear the case in case any dispute arises?*

[11] *Id.* at 10.
[12] Hague Convention on choice of court Agreement

The above situations reflects three considerations :

First, what is valid excusive choice of court clause?

Second, how can the place of business activity be determined when transaction is done online with foreign countries?

Third, which law shall govern the choose of court clause?

6.2.2 Scope of 'Choice' under the Hague Convention of Choice of Court Agreement

The Convention on Choice of Court established uniform rules for the application of the choice of law clause in international law. Aiming to promote international trade and investment through enhanced judicial cooperation.[13] The Convention applies solely to international cases of exclusive choice of court agreements concluded in civil or commercial matters. That is, it applies only to business-to-business (B2B) transactions.[14] It excludes application to consumer agreements.[15] However, this does not indicate whether it also excludes a large number of small and non-profit organizations. In addition, Article 2 (2) precludes its application to the carriage of passengers and goods, to claims for personal damage on behalf of or on behalf of national persons, and to other such matters. Article 10 further clarifies that a decision given in a closed matter pursuant to Article 2 (2) shall not be recognized or enforced under this Convention.

The general scope of the Choice of Court Convention outlined in Article 1 reflects its applicability to the digital age, as the international feature of the Convention since it strongly supports global cross-border electronic transactions. In addition, recognition and application of choice of court clauses concluded electronically can be also be found in two more articles of the Choice of Court Convention. Article 3(c) expressly states that an exclusive

[13] Paragraph 1 of the Hague Convention on Choice of Court Agreements.
[14] Hague Convention on Choice of Court Agreements, art. 2(1)
[15] *Ibid.*

choice of court agreement must be concluded or documented "in writing; or by any other means of communication, which renders information accessible so as to be usable for subsequent reference". The wording of this provision was inspired by Article 6(1) of the UNCITRAL Model Law on Electronic Commerce 1996. The terminology "by any other means of communication" should be deemed to include any electronic means, although this article could be made clearer by providing that "any communication by electronic means which provides a durable record of the agreement shall be equivalent to writing".[16] The consideration of electronic communications is also implied in Article 13 of the Choice of Court Convention. For example, Article 13(l)(b) provides that "the party seeking recognition or applying for enforcement shall produce the exclusive choice of court agreement, a certified copy thereof, or other evidence of its existence". The wording "or other evidence of its existence" was included mainly for agreements concluded electronically.[17]

6.2.3. Meaning of *Exclusive Choice of Court Agreements*

The definition of exclusive choice of court agreements in the Choice of Court Convention, laid down in Article 3, provides that:

(a) exclusive choice of court means an agreement concluded by two or more parties that meets the requirements of paragraph (c) and designates, for the purpose of deciding disputes which have arisen or may arise in connection with a particular legal relationship, the courts of one Contracting State or one or more specific courts of one Contracting State to the exclusion of the jurisdiction of any other courts;

(b) a choice of court agreement which designates the courts of one Contracting State or one or more specific courts of one Contracting State shall be deemed to be exclusive unless the parties have expressly provided otherwise.

---

[16] Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters ("Brussels I Regulation"), art.23(2) OJ L 012, 16.01.2001, p. 1 , *Available at* europa.eu.int/ eur-lex/pri/en/oj/dat/2001/01220010116en00010023 cited by Faye Fangfei Wang *Internet Jurisdiction and Choice of Law: Legal Practices in The EU,US and China* 22(Cambridge University Press 1st edition 2010)

[17] *See* Int'l Shoe Co. v. Washington, 326 U.S. 310 (1945) (explaining how the long-arm statute gives courts authority to assume jurisdiction over non-residents).

The above-explained Article 3 refers that the Choice of Court Convention only applies to the choice of court agreements in favour of the Contracting States, which can apply to both past and future disputes. It includes five requirements:

first, the agreement between two or more parties must exist;

second, the form requirement must be satisfied;

third, the agreement must designate courts of one state or one or more specific courts in one state excluding all other courts;

fourth, the designated court or courts must be in a Contracting State;

fifth, the designated courts must be connected to a particular legal connecti

In accordance with the above five necessities, there are three possibilities essential for exclusive choice of court agreements:

- It can refer to the courts of a Contracting State (e.g. the courts of the United States);
- It can refer to a *specific* court in a Contracting State (e.g. the Federal District Court of Texas);
- It can also refer to two or more specific courts in the same Contracting State (e.g. either the Federal District Court of Texas or the Federal District Court of California).

On the other hand, if two courts in different Contracting States were selected, for example, the courts of the United States and the courts of Australia, the choice of court agreement would not be measured exclusively under the Choice of Court Convention.

In accordance with the above requirements, there are three possibilities defining exclusive choice of court agreements: it can refer to the courts of a Contracting State (e.g. the courts of the United States); it can refer to a specific court in a Contracting State (e.g. the Federal District Court of California); and it can also refer to two or more specific courts in the same Contracting State (e.g. either the Federal District Court of California or the Federal District Court of New York). However, if two courts in different Contracting States were selected, for example, the courts of the United States and the courts of the United Kingdom, the choice of court agreement would not be considered exclusive under the Choice of Court Convention.

In a simple way, there are four basic rules under the Choice of Court Convention:

First, the chosen court must hear the case when proceedings are brought before it, that is, a court designated in an exclusive choice of court agreement "shall not decline to exercise jurisdiction on the ground that the dispute should be decided in a court of some other state".[18]

Second, any court not designated in the exclusive forum selection agreement must refuse jurisdiction.

Third, state parties must recognise and enforce judgments resulting from an exclusive choice of court agreement. [19]

Fourth, an optional provision allows states to declare that they will recognise and enforce judgments rendered by courts of other Contracting States designated in non-exclusive choice of court agreements.[20]

[18] The Hague Convention on Choice of Court Agreements, art. 5(2)
[19] The Hague Convention on Choice of Court Agreements, art. 8
[20] The Hague Convention on Choice of Court Agreements, art. 22

6.2.4 Jurisdiction and obligations in Court of Choice Agreement

Article 5 of The Choice of Court Convention describes which Courts will have jurisdiction in the case of courts of choice and in the absence of choice. Article 5 of the Choice of Court Convention serves to inform the chosen court how to respond to an exclusive choice of court agreement, while Article 6 provides the rule applicable to courts that are not chosen.

Article 5 establishes the basic rule that the court chosen by the parties in an exclusive choice of court agreement "shall have jurisdiction". Article 5 (1) states that the courts of a Contracting State designated in an exclusive electoral agreement will have jurisdiction to decide what the agreement applies to unless the agreement is null and void in accordance with state law.

Article 5 (2) reinforces the obligation under Article 5 (1) by stating that "a court having jurisdiction under paragraph 1 cannot refuse to exercise jurisdiction on the basis that the dispute must be decided in a court of another state". It means that if the parties choose "the courts of England" then the "courts of Scotland" will have no jurisdiction because England will be considered as the relevant territorial unit, while Scotland will be considered as an altogether other "state" for this purpose. However, if the parties choose "the courts of the United Kingdom", both the "courts of England" and "the courts of Scotland" can hear the case because "state" here refers to the United Kingdom.

In addition, Article 5 (3) states that the preceding paragraphs shall be without prejudice to the rules: a) on the jurisdiction of the object or value of the claim; b) on the internal allocation of jurisdiction between the courts of a State. However, when the chosen court has the power to decide whether to transfer a case, the choice of the parties must be duly taken into account. This article clarifies that the rules of the Convention govern only international jurisdiction and that private parties cannot create jurisdiction in the matter that otherwise does not exist in a national legal system. In addition, the Convention clearly affirms the lies about the internal division of jurisdiction in the contracting

States. Article 6 provides that the court of a Contracting State other than the chosen shall suspend or reject procedures to which an exclusive court choice agreement applies unless one of the following five exceptions occurs:

i) Null agreement and invalid according to the law of the chosen court;

ii) The inability of the party;

iii) Injustice manifestly or manifestly contrary to public order

iv) Uncontrollable factors; and

v) The chosen court has decided not to listen to the case.

For example, *A, who is a resident in Texas, sells goods to B, who is resident in Mumbai. B then resells goods to C who is resident in Beijing. The contract between A and B contains a choice of court clause in favour of the courts of Texas, whilst the contract between B and C contains no choice of court clause. Under these circumstances, B can sue A in Texas if necessary. C can sue B and A at the same time in London if disputes arise, because there is no choice of court agreement between A and C. But if C only sues B in London, B will not be able to join A as a third party, because the choice of court agreement* is *only binding between A and* B.

In above said example the Article 6 of the Choice of Court Convention, the court in London would have to suspend or dismiss any proceedings that *A* brings against *B*. The 'null and void' rule is the reverse of the exception to the obligation of the chosen court to assume jurisdiction in Article 5(1). If indeed the chosen court is not obliged to assume jurisdiction, then other courts should not be obliged to decline jurisdiction. Thus, Article 6 is set up for the purpose of ensuring that the court seized and the chosen court gives constant judgments on the validity of the choice of court agreements.

6.3 Internet Jurisdiction in the USA

In the US, in 2006, the American Bar Association (ABA) urged the Government to sign, ratify and implement the Choice of Court Convention for the reasons that it would make contracting parties more willing to designate litigation instead of arbitration and meet the need in transnational transactions for the enforceable choice of court agreements.[21] On January 19, 2009, the United States finally signed the Choice of Court Convention. This was the first signing of the convention and it appears that the United States is trying to take the lead and encourage others to accept the new harmonization regime.

Execution of US decisions in a foreign country is complex and has a very low success rate. If the US litigant seeks recognition and enforcement of the judgment in other nation courts, he must join a bilateral treaty of multinational Convention in this regard. This condition is not only limited to the United States, but is true for all nations since when a country seeks to impose the recognition of the judgment of its own countries court upon another country it needs to first enter into an agreement in that regard with the concerned country since under international law it is mandatory to seek mutual consent of both nations as the judgment of the court of one country is otherwise inapplicable on the other country.

In the United States, subject matter jurisdiction deals with the court's authority to hear and decide cases in certain areas of the law. Personal jurisdiction is the court's authority over a defendant and arises only when a defendant has sufficient ties to a state that makes him answerable to that state's courts. When a connection is found between the defendant and the state, the defendant is served a summons, or notice, about the lawsuit pending against him. Most states have long-arm statutes that set the state's guidelines for when its courts can assume jurisdiction over a non-resident defendant.[22] To comply

[21] American Bar Association Recommendation adopted by the House of Delegates, 8 August 2006, that the American Bar Association urges the United States government promptly to sign, ratify and implement the Hague Convention on choice of court agreement.
[22] *Id.*at 17.

with due process concerns, personal jurisdiction cannot offend traditional notions of fair play and substantial justice.[23]

Generally two kinds of the jurisdiction in USA on which state courts may exert jurisdiction are as follows:

- **i)** General jurisdiction
- **ii)** Specific jurisdiction

General jurisdiction is asserted over a non-resident defendant only if the defendant's contacts with the state are "continuous and systematic", even if the contacts are unrelated to the dispute at hand.[24] Specific jurisdiction arises when the lawsuit is related to the defendant's contacts with the forum state.[25] Both kinds of jurisdiction are relevant to internet law since it involves an *"in rem"* jurisdiction. Another area that is technically not pure jurisdiction, but is closely related, involves the requirement to meet the criteria as a foreign corporation to do business in a given state. Personal Jurisdiction in cyber cases refers to a growing series of judicial precedents in US courts where parties have declared personal jurisdiction based solely on their Internet activities. Personal jurisdiction in American civil procedural law is based on the idea that a defendant should not be subject to decisions of foreign or non-state courts, without "explicitly having recourse" to the advantages offered by the forum state.

The courts should defend defendants against the undue burden of litigation in an unlimited number of distant jurisdictions (in accordance with the requirements of the relevant constitutional process) the courts should prevent allegations of violation. Sovereignty of another state by limiting the by limiting the circumstances in which the "accused" can be brought to justice. By contrast, a specific personal jurisdiction allows a defendant to be sued in a

---

[23] *Id.*at 8.

[24] *Specht* v. *Netscape Communications Corp.*, 150 F. Supp. 2d 585 (SDNY 2001**)** affd,306 F.3d 17 (2d Cir. 2002).

[25] Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU,US and China* 164 (Cambridge University Press2010)

forum solely on the basis of his contacts with the forum. A court can establish a specific jurisdiction against a defendant only if it has "certain minimum contacts" that will rise to the action in question before the court so that the exercise of "non" jurisdiction does not violate the traditional notions of fair play and substantive justice. Cyber activities with a defendant outside the state usually require the plaintiff to assert a specific personal jurisdiction.

6.3.1 Jurisdiction in Cyber Cases in the USA

To assess the assertion of personal jurisdiction in Internet cases, courts applied both traditional and unconventional criteria and standards adapted to the online world. In 1945, the United States Supreme Court decided in the case of International Shoe v. Washington, 326 US 310 (1945), observed that in order for an accused to be called to court in a particular jurisdiction, he had to have at least a minimum level of contact with that state he could reasonably expect. Some important case law decided by Supreme Court of America is as follows:

i. The "Effects" or "Calder" Test: *Calder v. Jones Case*

The American Supreme Court in the case of *Calder v. Jones*[26] analysis the effects test of internet jurisdiction. In this case actress, Shirley Jones brought an action in a California court against the National Enquirer's Iain Calder and John South for an allegedly libelous article they wrote and edited in Florida. The article was published in the National Enquirer and distributed throughout California and the United States. In deciding to uphold California's personal jurisdiction over Calder and South, the Supreme Court concluded that "the fact that the actions causing the effects in California were performed outside the State [should] not prevent the State from asserting jurisdiction over a cause of action arising out of those effects." The Court accordingly held that defendants are subject to personal jurisdiction in a forum when they were "primary participants in an alleged wrongdoing intentionally directed at a

[26] *Calder v. Jones*, 465 U.S. at 784.

forum resident" and they knew their actions would injure the resident in the forum. Although some articles view Calder's effects test favorably and encourage its use when determining personal jurisdiction in Internet cases, more believe the standard should be modified. These articles offer a variety of solutions to perceived problems with the test. For example, one author claims Calder's "express aiming" or "purposefully directed" requirement "prevents the exercise of personal jurisdiction in cases where Internet based activities represent the modern functional equivalent of actual physical presence in a forum." The author suggests discarding that element and finding personal jurisdiction when defendants "engage in activity that will cause harm somewhere, no matter 'where that where may be.'" On the other hand, another author argues that "courts should require a higher burden of jurisdictional proof in effects test cases, even at the risk of limiting court access for some plaintiffs." This change would result in a more consistent application of the test and greater predictability for courts and defendants alike.[27]

However, in the emblematic case of *International Shoe v. Washington, the Court*[28] reduced the requirement of the physical presence of the defendant. The court held that two conditions must be met to assert:

a) The defendant has minimum contact with the forum state, which is the quality and nature of the defendant's action with regard to the right and orderly application of laws.
b) The process should not violate the traditional notion of fair play and justice under the Constitution.

Subsequently, the Apex Court in the case of *World Wide Volkswagen Corporation vs. Woodson*[29] added the concept of foresee-ability in the form of minimal contact to protect the defendant's right. The predictability test requires that if the defendant deliberately made use of the privileges cases in the forum

[27] Internet jurisdiction in united states *available at* https://www.fordham.edu (last visited on 28/02/2020)
[28] 66 S. Ct. 154 (1945).
[29] 444 US 286: 100 S. Ct. 559 (US Supreme Court, 1980).

state, and therefore regarding the cause of the action resulting from these activities, the court has jurisdiction. Therefore, if the defendant intentionally used or facilitated trade or services in the foreign State by any mode except his physical presence, he can't escape the jurisdiction of the Court.[30]

Further the Court extended the minimum contact theory in case of internet with the theory of sliding scale in the case of *Zippo Manufacturing Company v. Zippo Dot Com.*

ii. ***Zippo Manufacturing Co. v. Zippo Dot Com, Inc case***[31]

One of the most significant developments has been that of the "Zippo Continuum", or sliding scale of contact as delineated by the District Court in the Western District of Pennsylvania in *Zippo Mfg. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997).

This is a leading case on the internet jurisdiction of USA federal court. The decision of this case is called the Zippo test case. The fact of this case, Zippo involved a trademark dispute between Zippo Manufacturing, the Pennsylvanian maker of Zippo lighters, and Zippo Dot Com, a California- based Internet news service and owner of the "zippo.com" subscription news website. After being sued in federal court in Pennsylvania, Zippo Dot Com moved to dismiss the suit for lack of personal jurisdiction. Zippo Dot Com had approximately 3,000 paying subscribers in Pennsylvania and "agreements with seven Internet access providers in Pennsylvania to permit their subscribers to access its news service. Its additional contacts with Pennsylvania, however, occurred "exclusively over the Internet." The district court thus focused on whether it had specific, rather than general, personal jurisdiction over Zippo Dot Com.

After reciting the requirements for exercising specific personal jurisdiction over a non-resident and after briefly reviewing the major personal

[30] Jurisdiction of the Court, *available at* https://epgp.inflibnet.ac.in (last visited on March 27,2020)
[31] 952 F. Supp. 1119 (W.D. Pa. 1997).

jurisdiction case law, the district court concluded that “the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. The court described this proportionately as a sliding scale and stated:

At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign territorial jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet website which is accessible to users in foreign territorial jurisdictions. A passive website that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive websites where a user can exchange information with the host computer. In these cases, the exercise of personal jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.

Using this sliding scale, the district court found that Zippo Dot Com purposefully availed itself of the Pennsylvania forum by entering into electronic contracts with Pennsylvania residents. The exercise of personal jurisdiction was according to the court, therefore, proper.

The Zippo case decision has been cited by many courts as a standard of analysis for personal jurisdiction with regard to the Internet, but it has also undergone criticism. Zippo provides little guidance as to how much interactivity or commercialism is enough to justify intentional use. Furthermore, courts have given little direction as to how those factors interact. Additionally, there is no consideration built into the Zippo test for limiting the number of jurisdictions established. Once a website is sufficiently commercial and interactive beyond a threshold set by a court, jurisdiction may be established with every state.

6.4 Internet Jurisdiction in the European Union

The EU approach to internet jurisdiction is markedly different from the U.S. approach in that it is highly regulatory. The EU already suffers from a lack of skilled information technology (IT) workers. It is a phenomenon partially attributed to the lack of incentive for Europeans to aggressively upgrade their job skills since they are guaranteed a comfortable minimal standard of living from the social safety net of benefits the EU countries provide.[32] EU approach has been to establish a series of bright-line rules, this Section will only focus on B2C consumer transactions over the internet, as addressing all commercial transactions would be too huge of a topic.

In Europe, not many case laws are available on the aspect of jurisdiction on the Internet. For this reason, the law must inevitably be invoked. Since most legal systems in Europe are civil law systems, solutions based on the law should not be overlooked. There is no specific law of internet jurisdiction in the E.U. legal system. Rather, it is necessary to resort to more general international or national laws concerning matters of jurisdiction. With regard to trade matters in a European context, the main non-national bodies governing the competence to be established and the competence to adjudicate are the following:

a) The Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters

b) The Rome Convention on the Law Applicable to Contractual Obligations

[32]Marcus Franda, *Governing the internet: the emergence of an international regime* 89 (Lynne Rienner Publication 2001).

6.4.1 Brussels Convention

The Brussels Convention, 1968[33] deals with questions of jurisdiction and the enforcement of foreign judgments. Instead of legislation becoming automatic, member states of the Convention should enact laws in their own countries that would make the objectives of the Convention effective. According to the Brussels Convention, in a typical commercial transaction, the plaintiff would prosecute "performance of the obligation in question" or when the transaction has been completed or should have been completed. Article 13 of the Brussels Convention defines a consumer contract as a B2C contract for goods and services for purposes beyond the occupation or normal profession of a consumer if he meets the following conditions:

1. the contract was for the sale of goods on instalment credit terms; or
2. a contract for a loan repayable by instalments, or for any other form of credit, made to finance the sale of goods; or
3. any other contract for the supply of goods or services.

In addition, the conclusion of the contract should be preceded by a specific invitation addressed to the consumer or an advertisement in his State of domicile and the consumer had to take in his state of domicile the steps necessary for the conclusion of the contract. Article 14 gave the consumer a choice of jurisdictions between either his own domicile or that of the supplier (e.g., website owner). This bright-line rule left little room for discussion. If the contract met the conditions of a consumer contract, the consumer had the option of determining the jurisdiction in which to litigate. A consumer could also choose to forgo the choice of jurisdiction by opting to make an agreement with the supplier as to which court would have jurisdiction before agreeing to the contract in a forum selection clause. This opt-out choice was allowed only if it fulfilled several formal requirements. The agreement had to:

[33] Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, 1968 O.J. (C 27) 1 [hereinafter Brussels Convention]

1. Be in writing;
2. Be in a form that conformed to practices established between the parties; and
3. In international trade or commerce, be in a form that accorded with the usage of a certain dignity.

Still, jurisdiction was an entirely separate story for suppliers (e.g., sellers). In a restriction against suppliers, Article 14 only allowed suppliers to bring suit in a consumer's domicile. The limitation against suppliers further applied to non-EU suppliers who had branch offices in the EU, The Brussels Convention certainly favored consumers in its jurisdiction provisions.

6.4.1.1 Brussels I Regulation

While the Brussels Convention acutely dealt with jurisdiction, it had not anticipated the internet and the unique difficulties that e-commerce would cause courts in ascertaining where a case should be heard. As seen in Section 4.1, merely establishing the domicile of an internet user could be difficult. Furthermore, e-commerce in the EU clearly lagged behind the United States and much of this was attributed to a lack of consumer confidence in the security of internet transactions. As a result, on 22 December 2000, the EU's Council of Ministers adopted Brussels I Regulation in an effort to modernize the Brussels Convention. Brussels I came into force in March 2002.

Brussels I differed from the Brussels Convention in adoption, for it was directly binding on the members of the EU, rather than having each country adopt its own version in its statutory code there was great debate over whether Brussels I would take a country-of-origin or country-of-destination approach in consumer transactions. The country-of-origin approach dictates that all legal disputes over transactions contracted over the internet would be determined by the law of the supplier, where the good/service originated. Consumers are thought to be disadvantaged by this approach because the approach subjects them to foreign laws they may not be familiar with when purchasing a product in another member state of the EU. This problem is only compounded if the seller masks his domicile on his website. The country-of destination approach applies the law of the consumer's domicile in legal disputes over internet transactions. This is advantageous for consumers, but it leaves sellers vulnerable to being subject to any foreign jurisdiction where their web site can be accessed.[34]

Furthermore, Brussels I makes it clear that contracts completed via an interactive website falls within its confines, thereby giving every EU consumer who buys a good/service through the internet the privilege of litigating in their own domicile. The consumer's freedom to choose which domicile to bring a cause of action is significantly strengthened. Brussels I also retained the Brussels Convention limitation that restricted a supplier's choice-of-law to bringing suit in the consumer's domicile. Lastly, while Article 17 in Brussels I allows for forum selection clauses, it does not allow any such contractual agreements to take away the consumer's right to bring suit in his home jurisdiction unless the agreement is entered into after the dispute arises. Ultimately, if a seller is running a web site that is 'directing its activities' towards an EU member state, under Brussels I, the seller would be under that member state's jurisdiction. Brussels I unabashedly protects the consumer's choice of forum by embracing the country-of-destination approach.[35]

Article 23 of the Brussels I Regulation authorizes the parties to conclude an agreement designating the court or courts responsible for settling these disputes. Article 23 (1) applies where at least the parties, one or more of whom are domiciled in a Member State, have agreed that the courts of a Member State must have jurisdiction to hear disputes arising from a legal relationship. Particularly, the parties can choose courts or tribunals specific to a country. For example, business.

[34]Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters 1968, *available* at https://www.jus.uio.no (last visited on June 8, 2021)
[35] *Id.* at 17.

In the case of *WH Martin Ltd* v. *Feldbinder Spezialfahzeugwerke GmbH*[36]

A (in Italy) and Company B (in Germany) have agreed a jurisdiction clause "disputes must be referred to the courts of Germany" in their electronic contracts of sale. Under these circumstances, German courts are designated to have jurisdiction over A and B's disputes. However, if later on A and B made another distribution contract without a jurisdiction clause (the sales contracts and the distribution agreement are different legal relationships), then the original jurisdiction clause in the sale contract does not confer jurisdiction with regard to a dispute arising under the distribution contract

If the jurisdiction clause includes a choice of a particular court, Article 23 operates to confer jurisdiction on that court, but not on other courts in the same country. However, party "A" and party "B" can also choose the other courts, for instance, the French court instead of the Italian or German courts, to hear the case because Article 23 does not "require any objective connection between the parties or the subject matter of the dispute and the territory of the court chosen".

6.4.1.2 Rome Convention on the Law Applicable to Contractual Obligations

While the Brussels Convention and Brussels I deal with which court has jurisdiction over a case, The Rome Convention, 1980 (Rome I) deals with the substantial choice of the applicable law. It allowed consumer contracts to include a forum selection clause, provided that the consumer has not been refused protection of the local consumer law. This consumer protection has been authorized, provided that the contract has been preceded by an advertisement or invitation addressed to the consumer or Member State of the consumer and that the contract was concluded in the consumer's domicile. In a similar movement to update Rome I, The EU has drawn up a proposal, Rome

[36] [1998] ILPr 794.

II, the aim of which is harmonize Member States' rules on conflict of laws. While Rome I applied to both contracts and non-contractual contracts, Rome II only applies to non-contractual matters. More specifically, Rome II would apply to cross-border liability disputes in which there are no contractual matters. Its tentative proposal takes a destination country approach and enforces the law. The country where the injured party (requesting consumer) resides in a non-contractual obligation, consumer's choice of forum by embracing the country-of-destination approach will be applied.[37]

Rome II, or the Rome regulation on the law applicable to non-contractual obligations, has been applied since January 11, 2009. It permits the parties to contractually agree on a governing law for non-contractual obligations. It is not limited to damages or only to non-contractual obligations recognized in English law. In addition, certain claims filed in tort under English law may not be included in Rome II, but in Rome, I and may be subject to the choice of contract law rules. Rome II applies to situations involving a conflict of laws in civil and commercial matters. Special rules are established for non-contractual obligations in the event of damage caused by defective products, damage resulting from an unfair commercial practice, violation of the environment and violation of intellectual property rights.

Rome II also applies to pre-emptive actions. These are defined in the regulation as:

- non-contractual obligations that are likely to arise;
- events giving rise to damage that are likely to occur;
- damage that is likely to occur.

Certain matters are excluded, including:

- revenue, customs, and administrative matters;

[37] Proposal of Council Regulation on the Law Applicable to Non Contractual Obligations, (Rome II) art. 3

- obligations arising out of family relationships and matrimonial property issues;
- negotiable instruments;
- company law issues;
- voluntary trusts;
- nuclear damages;
- defamation and privacy;
- evidence and procedure.

6.4.2 *LICRA c. Yahoo* [38]: A landmark case on Cyber Jurisdiction

This was a landmark case on cyber jurisdiction between the US and France. The facts of this case were as follows:

On May 22, 2000, the Superior Court of Paris, at the request of the UEJF and LICRA, condemned Yahoo!, Inc. (hereinafter "Yahoo! US") and the Yahoo! France (hereinafter referred to as "Yahoo! France") and directed to adopt a series of measures aimed at (i) preventing the sale of material related to Nazism on Yahoo! and (ii) warn users that Yahoo! It may contain links to elements and information prohibited by French law. Yahoo! US and Yahoo! France challenged the order, arguing that it was technologically impossible to comply with it. On November 20, 2000, the Superior Court of Paris confirmed its previous decision and issued a new order fixing a deadline of 3 months for the execution of its decision.

On December 21, 2000, Yahoo! US has filed a lawsuit against the UEJF and LICRA in the United States District Court for the northern district of California in San Jose. Yahoo! US requested a declaratory judgment establishing that orders made by the High Court of Paris are not recognizable or enforceable in the United States because they violate the first amendment to the United States Constitution. On June 7, 2001, the district court issued its order dismissing the dismissal motion and stated that it had jurisdiction over

[38] Scottish Daily Record (Apr. 13. 2000) 41.2000 WL 17093040.

the UEJF and LICRA. On November 7, 2001, the district court issued its order for summary judgment declaring that "the first amendment prohibits execution in the United States."

UEJF and LICRA appealed the District Court's decision claiming that:

1. the District Court lacked personal jurisdiction;
2. the case was not ripe **-** i.e. it was contingent upon a future condition, the request to enforce the French decision in the US, and
3. the District Court should apply the abstention doctrine, which prevents a court from deciding on a case because it would intrude upon the powers of another court.

On 23 August 2004, the US Court of Appeals for the Ninth Circuit affirmed that the District Court lacks jurisdiction and reversed the decision without addressing the other two claims. However, the Court of Appeals decided to rehear the case en banc and, on 12 January 2006, reversed the previous District Court's judgment, remanded the case and ordered to dismiss the action. On 30 May 2006, the Supreme Court denied LICRA's request to issue an order to review the judgment (certiorari).

Commentary and Some Important Points of the Yahoo Case

This case raises a number of issues regarding the legitimacy of restrictions on freedom of expression and the territorial applicability of national laws. On the first point, the American legal system does not include provisions such as article R645-1 of the French penal code. This provision prohibits the wearing or display in public uniforms, badges or badges connected, among other things, to Nazism and the Third Reich.[39]

This provision is in line with Article 5 of the Declaration of Human Rights and the Citizen which authorizes restrictions on freedom of expression when they are necessary to avoid society. On the contrary, the first amendment

[39] Rodney D Ryder, *Introduction to Internet Law and Policy* 76 (Wadhwa and Company New Delhi2007)

of the US Constitution expressly states that Congress will not enact any law "which restricts freedom of expression". Consequently, restrictions on freedom of expression are extremely limited (such as obscenity or defamation) and do not include the sale or display of goods relating to Nazism. In relation to the second problem, the territorial applicability of the laws, the transnational nature of online communication presents a major challenge to the concept of jurisdiction as traditionally envisaged.[40]

Websites are potentially accessible to anyone with a device connected to the Internet, regardless of their geographic location. Asserting jurisdiction over website operators on the grounds that their websites are accessible in this country would encourage website operators to comply with the laws of all countries where their websites are accessible. Another approach would be to apply the "country of origin" principle, requiring website operators to comply only with the laws of the country in which they are established. However, applying the "country of origin" principle would create new challenges, such as creating websites in less restrictive jurisdictions to avoid prosecution for illegal activities.[41]

There is significant criticism of the country-of-destination approach adopted in Brussels I and the draft proposal of Rome II. Because this approach subjects sellers to increased litigation costs, sellers may be tempted to pass these costs on to consumers by way of higher prices. Sellers may also choose to decrease the number of choices available to consumers by limiting the use of their web sites to certain consumers through closed computer systems, or by simply shutting down their web presence. For an example of increased litigation harassment, in Germany, consumer protection groups such as the Federation of German Consumer Organizations ("VB") surf the web to see which web sites are not in compliance with the new laws that regulate distance

[40] *Id.* at *39*

[41] Yahoo case on cyber jurisdiction *available* at https://www.google.com/search?q=yahoo+cases+cyber+jurisdiction&oq=yahoo&aqs=chrome .0.69i59l2j0j69i57j0l2j69i60l2.4504j0j9&sourceid=chrome&ie=UTF-8# (last visited on March 1,2020.)

sales. Then, VB sues the web site companies for failing to meticulously comply with regulations in which the web site owners are not well-versed.[42] It does not even matter if the web site does not sell anything.[43]

6.4.3 A Comparison of U.S. and European Approaches to Internet Jurisdiction

While the United States has relied on its courts and the EU has relied on legislation to determine jurisdiction in cases involving consumer Internet transactions, each approach has significant weaknesses which are greatly compounded when a transnational approach is attempted for consistency. The fundamental weakness of the American approach is its lack of predictability Unlike the clear line rules set out in the EU, companies need to interpret whether or not their websites reach the level of interactivity that the courts will consider sufficient for a minimum contact because court decisions are the only measure by which businesses must pass the childhood of e-commerce. This means that the two current tests, Zippo Continuum and effects-based test or the bright-line rule are unlikely to be permanent. Therefore, Thomas Vartanian, former President of the Global Cyberspace of the American Bar Association Skill Project noted**:**[44]

"Anyone doing business in cyberspace needs to know what laws to obey, whether it be a question of what taxes are due and where, or what consumer protections apply to the sale of their products or services.... [A] legal infrastructure that can provide the requisite elements of certainty and predictability.. .will allow electronic commerce to flourish as efficiently as market forces dictate."[45]

---

[42]Brussels I and the draft proposal of Rome II , *available* at https://www.law.upenn.edu (last visited March 9,2020)

[43] *Ibid*

[44] *Supra* note at 39, pg 55.

[45] ABA Group Releases Study on Internet Jurisdiction; Ground-Breaking Report Calls for the Creation of a Multinational Jurisdiction Commission, Encourages New Forms of Online Dispute Resolution, PR Newswire ,July 10,2000, *available* at http://library.northemlight.com.

Because the United States depends on its private sector to stimulate the limits of what should and should not be regulated in this Internet sector,[46] legal standards are constantly evolving.

While the Brussels I proposal and the EU Rome II (regulation on the law applicable to non-contractual obligations) emphasize on clear rules for transactions with consumers, this regulatory approach still has significant weaknesses. First, laws, as written, remain ambiguous in their interpretation when applied to the Internet. Second, the destination country approach hampers the growth of e-commerce in the EU, which is precisely the opposite effect envisaged by the EU.[47]

Michael Cordera, in his commentary, titled E-Consumer Protection: A Comparative Analysis of Consumer Protection in The EU and The United States, argues that Brussels II editors misunderstood the nature of electronic transactions with consumers and then wrote too broad a regulation in the form of Brussels II, when they adopted the country of destination approach.[48]

There are important criticisms of the country of destination. The approach adopted in Brussels I and Rome II. Because this approach puts sellers at higher litigation costs, sellers may be tempted to pass these costs on to the consumers by way of higher prices. Sellers can also choose to reduce the number of choices available to consumers by limiting the use of their website to certain consumers through closed computer systems or simply close to your web presence.[49]

While The EU approach significantly affects small and medium-sized businesses that can watch the Internet as the perfect means to grow their businesses. Large conglomerates operating throughout the EU or worldwide

---

[46] The White House, *A Framework for Global Electronic Commerce* (July 1, 1997)

[47] Brussels Convention on jurisdiction Available at https://www.google.com/search?q=brussels +convention+on+jurisdiction&oq=brusells+convention+on+&aqs=chrome.1.69i57j0l7.23912j0j7&sourceid=chrome&ie=UTF-8# (last visited on March 2, 2020)

[48] E-consumer-protection a comparative analysis of EU, *available* at https://www.questia.com /library/journal/1G1-81115387/ (last visited March 9,2020)

[49] *Id.* at 31.

can more easily afford legal experience to avoid the various legal difficulties involved in global practice. Small and medium-sized businesses do not have the same luxury and can choose to close their websites in light of the possibility of further litigation where the cost of a single lawsuit in a foreign jurisdiction can cause them to close.[50]

In short, the researcher concludes all debates between EU and US regarding cyber jurisdiction, both have a different legal system, US cyber jurisdiction based on judicial precedent and courts decisions while EU law on cyber jurisdiction made by statutes. The US provides a free environment for doing business on the internet due to the judicial system but the EU does not provide such an environment because the legislature makes law.[51]

After discussing the international framework regarding jurisdiction issues in e-commerce, the researcher will like to discuss about other international effort like Online Dispute Resolution (hereinafter ODR) to resolve jurisdiction dispute. ODR can be significant step from the perspective of system of solving of a dispute (the dispute may be offline or online).

6.5. Online Dispute Resolution

The word ‘online dispute resolution’ (ODR) can, on a prima facie screening, have two meanings. Firstly, it can be taken as a resolution of online disputes; it would mean resolution of online disputes. It would include the solving of (by any means, either online mechanism or offline method including court adjudication) disputes which essentially arises from an online transaction. This would include a dispute like a defect in computer software purchased online through an auction website where the payment was made online through a credit card and the software was immediately transferred to the consumer using the same online environment. Secondly, ODR may play a significant role as system of resolving of a dispute (be the dispute be offline or online). This

[50]Online dispute resolution for consumers in the EU, *available* at https://www.oapen.org/download/?type=document&docid=391038 ,(last visited on March 2,2020)
[51] *Id.* at 41.

means that newer ways of solving a dispute are being developed by making use of the online environment which can be applied to solve any kind of disputes. ODR in this context would include online negotiation, online mediation, online arbitration, online neutral evaluation, online peer jury, etc.[52]

Another concept to be borne in mind is the 'online environment'. The word 'online' has been popularly connected to the Internet, that is to say, anything available on the Internet is available 'online'. Despite, in the context of ODR, the digital environment has a wider implication in terms of a set-up making use of technology and communication facilities. It would include the use of telephone, fax, or e-mail facilities or any other mode available on the Internet or any other information and communication technology that can be beneficially used to solve disputes.[53]

This part of the chapter has focused on ODR as a tool for resolving any kind of dispute limited to the resolution of online disputes only. Hence, taking the system-based approach, ODR covers a variety of ways in which a party, by making use of the 'online environment', solves its dispute or clash of interests.

While ADR can work in an ad hoc environment, ODR necessarily requires an institutional backup. For a successful working of ODR, an institutional set-up is a must. This means there should be an organizational set-up which offers ODR services. It should have the following features:[54]

(a) A proper administrative infrastructure which would support the ODR services.

(b) A technically up-to-date and user-friendly computer interface with strong back-end support to enable the user to make the best use of the services being offered.

---

[52] S.K. Verma And Raman Mittal (eds.) *Legal Dimensions of Cyberspace*, 308 (Indian Law Institute, New Delhi, 2004)
[53] New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, *Available at* https://www.uncitral.org/pdf/english/texts/arbitration/NY-conv/New-York-Convention-E.pdf1958 (last visited on March 10,2020)
[54] *Ibid*

(c) A panel of arbitrators, mediators, etc. who are impartial and independent and enjoy the confidence of the industry at large which will be required using the services being offered.

It is of utmost importance that any institution providing ODR services should be able to generate trust and confidence among the users. Generating e-confidence has been a persistent problem since every person involved in internet services have been facing it. The primary reason for failure of many e-commerce websites offering various commercial services has been lack of trust. Unless there is an institutional backup in the physical world, expecting an exclusive online service is almost next to impossible, though there have been exceptions. The primary concern for any user of such online services is, apart from the authenticity and reliability of the service provider, possibility of fixing the responsibility on a single person in case of any deficiency of services. In such situation, not only the online service institution should be backed by an offline set-up, it should also follow the disclosure-based approach which further helps in creating e-trust and e-confidence among the users of the online system.[55]

6.5.1 The Legal Obstacles and Solutions to Online Arbitration and Online Mediation

Online Dispute Resolution (ODR) provides efficiency and convenience in resolving conflicts, but at the same time faces a number of challenges on account of technology, management and legal barriers.

The ODR is certainly much younger than most existing laws. The question of whether existing laws can provide a sufficient legal basis for cases resolved by the ODR is very controversial. It is also controversial whether the new laws should take into account provisions adapted to the new information technologies. The bottom line, however, is that the ODR has become a reality

[55]Guide to International Arbitration - Latham & Watkins LLP, *available* at: https://www.lw.com/ thoughtleadership/guide-to-international-arbitration-2017 (last visited on June 8, 2021)

due to its increasing use. The interpretation of the rules on the validity of electronic arbitration and mediation agreements as well as on the execution of electronic arbitration awards and settlement agreements differs from country to country. To encourage and allow the ODR to continue, legal obstacles must be removed.[56]

6.5.2. Online arbitration

Online arbitration is one of the most complicated ODR processes since its non-localization challenges the traditional concepts of “arbitration agreements”, “place of arbitration” and “place of arbitration awards”. This creates legal uncertainty regarding the validity, jurisdiction and applicable law as well as the enforceability of arbitration agreements and arbitral awards.

a) Validity

Traditionally, an arbitration agreement must be written. This is provided for in Article 2 of the 1958 Convention on the Recognition and Enforcement of Foreign Arbitral Awards (hereinafter The New York Convention).[57] The New York Convention has been adopted by most countries, including China, the United States, and the EU. It is considered to be one of the most successful conventions providing certainty for the recognition and enforcement of cross-border awards.[58]

Whether electronic arbitration agreements and awards can meet the requirements for these agreements and awards to be written form by the New York Convention. It is proposed that the digital awards if they can be printed and signed, meet the written requirements. However, if electronic conventions and arbitral awards can be treated as “electronic contracts”, their validity is automatically recognized by the United Nations Convention on the Use of

[56] Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU,US and China* 157 (Cambridge University Press 2010)
[57] New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, *Available at* https://www.uncitral.org/pdf/english/texts/arbitration/NY-conv/New-York-Convention-E.pdf 1958(last visited on March 10,2020.)
[58] *Ibid*

Electronic Communications in International Contracts and other national laws on electronic contractual laws. In some countries, conflict of law rules may include the determination of the validity of an arbitration agreement. In tradition, the legality of an arbitration agreement should be governed by the law preferred by the parties. In the unavailability of the parties' choice of law, the law of the place where the arbitration takes place or the award is made should apply. Such a law is proposed in Article 151 of the Draft Model Law of Private International Law in China (hereafter Draft China Model Law). The adoption of such a rule would definitely increase legal certainty. However, the determination of the place of arbitration in cyberspace would still face legal challenges.

b. Jurisdiction and applicable law

The place of arbitration or chair of arbitration is normally used to ascertain the application of the nation's arbitration law and later the nation of origin for enforcement purposes. The seat or place of arbitration shall be agreed by the parties. In the absence of such a choice, it can be problematic to identify the place of arbitration and this is even more difficult in the case of cyberspace since it lacks a physical location. In common practice, the place of arbitration in cyberspace shall be interpreted as the place of domicile of the chairman of the arbitral tribunal, the location of the place of business or the main server of the dispute resolution provider. In the researcher's view, "the domicile of the chairman of the arbitral tribunal" seems to be a more appropriate and effective connecting factor in determining the location of arbitral procedures such as "the location of the main server or establishment of the dispute resolution provider".

The latter contradicts the general principle of the determination of the location of the party in cyberspace according to Article 6 of the UN Convention on the Use of Electronic Communications in International Contracts. Similar to court litigation, parties are allowed to choose the applicable law for their contracts. However, such choice shall not infringe the mandatory rules or public policy of the country. Within the scope of application of party autonomy, arbitral tribunals do not have the power to disregard the parties' instructions as excess of power and procedural irregularity are both grounds for setting aside or refusing to enforce an arbitral award according to Article 34(2)(a)(iii) and 34(2)(a)(iv) of the UNCITRAL Model Law on International Commercial Arbitration and Article V(l)(c) and (l)(d) of the New York Convention.[59]

Beyond the scope of application of party autonomy, the parties' instructions do not have effect and do not limit the arbitral tribunal's power to determine the applicable law. Under such circumstances, the arbitral tribunal will determine the private international law (e.g. under the Brussels I Regulation and Rome I Regulation in the EU), and then the chosen rule/regulation of private international law will direct the appropriate jurisdiction and substantive applicable law.

The researcher would like to suggested that the parties should prefer the system of private international law that the arbitral tribunal shall use in order to avoid any ambiguous application and to create legal certainty as, in the absence of any reference to a private international law, there is no indication that the tribunal will apply a conflict rule to identify the proper law. In the meantime, if the arbitral tribunal decides to apply a conflict rule, it will face the same challenges of the determination of applicable law of electronic contracts as in court litigation.

In the choice of arbitration in practice, arbitration is carried out according to the procedural rules agreed by the parties, which do not violate the mandatory provisions of the law of the place where the arbitration takes place or the award has been rendered. In the absence of an agreement, the procedural rules laid down by the arbitral tribunal apply. These rules are set out in Article

[59] Article V - Guide - NYCG 1958 - 1958 New York Convention, *available* at: https://newyorkconvention 1958.org (last visited on June 8, 2021)

13 of the UNCITRAL Model Law on International Commercial Arbitration. It is challenging that online arbitral procedures might require different rules. For example, the Arbitration Court, and the Czech Republic has enacted “additional procedures for on-line arbitration (on-line Rules)” including definition, principles, calculation of time period, statement of claim, place, and notification of arbitral award relating to online arbitration. The American Arbitration Association has also introduced the “Online ICDR Protocol for Disputes between Manufacturers and Suppliers”.[60] But, those two procedures for online arbitration are very diverse in terms of the content and style. This raises concerns about the criteria of the legitimacy of online arbitration procedures.

c. Enforceability

ADR, in specific arbitration, is encouraged as the most proper method for resolving cross-border commercial disputes due to its time efficiency and flexibility in the meeting of expert arbitrators in relation to legal disputes. The parties who choose to arbitrate their disputes hope to reach an agreement or an arbitral award and to execute that award without recourse to a court. However, sometimes a losing party may present an arbitral award as a refusal to perform, or a winning party may request recognition and implementation of the arbitral award if the defeated party has not complied with the judgment.

Recognition and enforceability of an award is one of the most common complex issues in the traditional method of arbitration, because the court first decides its capability to recognize and execute an award and in exercising jurisdiction over the arbitral award depending on the location of the arbitration or the location of arbitral award; second, the court shall examine the validity of

[60] Established in 1996 as the international division of the American Arbitration Association, the International Centre for Dispute Resolution (ICDR) is one of the most recognized and prominent providers of international dispute resolution services in the world. Key to this success is our Case Management Team, comprised of highly trained professionals from around the globe who, in addition to an in-depth understanding of ICDR International Arbitration Rules and Mediation Procedures, have a proven track record for moving matters forward, helping to control costs, and respecting cultural differences.

the arbitration agreement in terms of its form, forum and arbitrators; third, the court shall evaluate the arbitrability of the dispute including the validity and extent of the content of the arbitration agreement in reference to the public policy of the preferred state.

The complexity of the recognition and enforcement of arbitration was highlighted in the European Commission's Report on the Review of the Brussels I Regulation on 21 April 2009, which stated that the Brussels I Regulation has in specific instances been interpreted so as to support arbitration and the recognition/enforcement of arbitral awards. The Green Paper that accompanies this Report further explains its scope and states that:

However, addressing certain specific points relating to arbitration in the Regulation, not for the sake of regulating arbitration, but in the first place to ensure the smooth circulation of judgments in Europe and prevent parallel proceedings.[61]

6.5.3. Consumer Protection and Arbitration

When arbitration is proposed for consumer contracts, a major legal obstacle is whether the arbitration agreement is valid or effective, as permitted by the law of the country of consumer protection, may be deemed to be unconscionable or an unfair term in the particular context. In other words, countries can limit the applicability of an arbitration agreement before a dispute against a consumer. For example, according to Article 91 (1) of the English Arbitration Law (hereinafter "EAA"), an arbitration agreement with a consumer is considered unjust and therefore unenforceable if the claim is below £5,000. It indicates that, in England, if the amount in dispute does not exceed £5,000, an arbitration clause with consumers is unnecessary. In the case

[61] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Council Regulation (EC) No.44/ 2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Brussels, 21.4.2009, COM(2009) 174 final, Commission of the European Communities, p.9, *Available at* www.ipex.eu/ipex/cms/home/Documents/ doc_COM20090174FIN (last visited on March 10,2020)

of Richard Zellner v. Phillip Alexander,[62] Securities and Futures Ltd the German court and the English Court of Appeal both assessed the validity of the arbitration agreement and held that the arbitration agreement was invalid as it was an improper term towards the consumer.[63]

However, in the US, it is arguable that an arbitration clause with consumers could be enforceable, as Section 2 of the Federal Arbitration Act (hereafter "FAA") 1925 is an open (minimum) clause stipulating that a written provision in a maritime transaction or a contract provides for a transaction in which the trade is settled by arbitration, any controversy resulting from such a transaction or contract is valid, irrevocable and enforceable. It will be up to the judge to determine the scope of "involving commerce". Sometimes an arbitration agreement before litigation is valid but not enforceable. Like in the case of *Allied-Bruce Terminix Cos v. Dobson*[64] the court decided that the phrase "involving commerce" is broad and was intended as the functional equivalent of affecting commerce. Seldom, the court also intends to protect consumers. In the case of *Brower v. Gateway 2000, Inc*,[65] the New York Appellate Court held that there was an arbitration agreement in the consumer dispute between the parties according to the Federal Arbitration Act. However, the arbitrator chosen was not fair to the consumer and thus the court asked the parties to find an appropriate arbitrator.

The Arbitration Fairness Act of 2009 (hereafter AFA) amends the FAA and invalidates pre-dispute agreements to arbitrate "franchise, consumer, employment or civil rights disputes. Thus, it prevents the use of compulsory pre-litigation arbitration clauses. The AFA has provisions of consumer protection. However, it does not propose new rules for arbitration agreements or procedures that are formed on the Internet. The interpretation of "written"

---

[62] *Richard Zellner v. Phillip Alexander Securities and Futures Ltd, Landgericht Krefeld Case* 1996 [1997] ILPr 716; [1997] ILPr 730 (QB) 736-8

[63] *supra* note at 8, pg 162.

[64] *Allied-Bruce Terminix Cos v. Dobson,* 513 U.S. 265, 273 (1995).

[65] *Brower* v. *Gateway 2000, Inc,* Supreme Court of New York, Appellate Division 246 A.0.2d 246 676 N.Y.S. 2d 569, 572 (1998).

arbitration agreements must, therefore, be reconciled with the electronic signature in the world and national law (E-SIGN). Therefore, electronic arbitration agreements are valid and enforceable for B2B contracts.[66]

According to the AFA, it should also be understood that no online pre-dispute arbitration agreement for B2C/consumer disputes shall be valid or enforceable. Currently, sellers or suppliers in a B2C e-commerce situation often include an arbitration clause in the standard consumer dispute form. It is unfair that consumers have no position to negotiate or argue with the arbitration clause. Once consumers click the "I agree" button, the contract is formed. With the amendment of the rules associating to pre-dispute arbitration agreements, such electronic pre-dispute arbitration agreements shall be invalid and void.

If parties form an electronic arbitration agreement for consumer disputes after the dispute arises, such an electronic arbitration agreement shall be agreed to by both parties in order to be valid. The case of Specht v. Netscape Communications Corp[67], the court ordered that the smart download software license agreement did not bind the plaintiffs and therefore refused to go to arbitration for them. Plaintiffs violation of the licence agreement, because Netscape's Smart Download (shrink-wrap agreement) permits a user to download and use the software without taking any action that plainly manifests assent to the terms of the associated licence or indicates an understanding that a contract is being developed.[68]

6.6. Online Mediation

Unlike online arbitration, most online mediations are provided by public bodies (e.g. AAA or CIETA), while a large number of online mediation services are provided by private companies. The quality of online mediation

[66] Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU,US and China* 163 (Cambridge University Press2010)
[67] *Specht* v. *Netscape Communications Corp.,* 150 F. Supp. 2d 585 (SDNY 2001) affd, 306 F.3d 17 (2d Cir. 2002).
[68] Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU,US and China* 164 (Cambridge University Press2010)

services and the internationally harmonized standard go a long way to increase users' confidence in online mediation.

This kind of ODR involves the dual process of negotiation and mediation consecutively. The parties can initiate the ODR process by opting online negotiation and make an attempt to negotiate their differences and reach at a settlement. In case they are unable to do it themselves, a mediator is appointed which conducts an online mediation and helps the parties reach a settlement. For example, SquareTrade.com provides individual and B2B buyers and sellers an online negotiation-cum-mediation environment. The complainant files a case with 'SquareTrade' by completing an online form that helps identify the situation and possible resolutions. The other party is notified by e-mail and responds to the case. Communication from both parties is posted on a private *case page*. Then direct negotiation begins. During direct negotiation, the parties communicate with each other in a confidential, impartial forum. If the case is not resolved, SquareTrade assigns a mediator from the Square Trade Network who helps the parties reach a mutually acceptable settlement.[69]

At present, the number of business transactions on the Internet platforms, so do complaints of poor service, poor manufacturing quality, and total fraud. The most recent challenge for conflict mediators is the resolution of these disputes, which often involve people who have never met. Alternative dispute resolution, which uses mediators rather than the court system to resolve disputes, has grown in demand as people seek long-term, cost-effective solutions to a suite of civil disagreements. As the number of online disputes increases, conflict mediators not only spend more time with you, but also develop new negotiation strategies tailored to "cyber conflicts", especially through email, instant messaging, and discussions.[70]

[69] S.K. Verma And Raman Mittal (eds.) *Legal Dimensions of Cyberspace*, 315 (Indian Law Institute, New Delhi, 2004)
[70] https://www.mediate.com/articles/ansonline.cfm (last visited on March 11,2020).

Website onlinemediators.com was launched in the year 2000 for online mediation. An established Internet-based mediation community with some 3,000 members. The center in its latest endeavour concentrates on business-to-business disputes and it also plans to generally advocate mediation as a way of building trust between online vendors and their consumers.[71]

In the EU, online mediation, as a form of out-of-court dispute resolution, is generally encouraged. Although there are no substantial ODR rules in the EC Directive on Electronic Commerce. It encourages ODR practice requiring the Member States to ensure that their laws "do not hinder the use of extrajudicial mechanisms, available under national law, for the settlement of disputes, including appropriate electronic means".[72] Furthermore, it obliges the Member States to "encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding Information Society services and to convey any other information on the usages, practices, or customs relating to electronic commerce.[73]

In addition, the EC Directive of the European Parliament and of the Council on Certain Aspects of Mediation in Civil and Commercial Matters (hereafter EC Directive on Mediation) was approved by the European Parliament on 23 April 2008[74] and entered into force in June 2008. The purpose of the EC Directive on Mediation is to facilitate access to dispute resolution, to encourage the use of mediation and to ensure a sound relationship between

[71] *Id.* at 70

[72] Directive 2000/31/EC of the European Parliament, Art. 17(1) and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market Commerce", OJ L178, 17.7.2000 pp. 1-16.

[73] EC Directive on Electronic Commerce. art. 17(3)

[74] Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters (hereafter "Mediation Directive"), OJ L136/5, 24.5.2008, *available* at eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri =OJ:L:2008:136:0003:0008: EN:PDF (last visited on 11 March 2020).

mediation and judicial proceedings.[75] It is considered to be an achievement in the regulation of out-of-court dispute resolution. It favours electronic communications and, to an extent, online dispute resolution. It encourages the use of mediation in cross-border disputes and the use of modern communication technologies in the mediation process, as evident in the recitals (8) and (9), which state as follows:

(8) The provisions of the EC Directive should only apply to mediation in cross-border disputes, but nothing should prevent the Member States from applying these provisions also to internal mediation processes.

(9) This Directive should not in any way prevent the use of modern communication technologies in mediation.

It should also be noted that the EC Mediation Directive includes the single "enforceability of agreements resulting from mediation" provision in Article 6 which provide as follows:

1. The Member States shall assure that it is possible for the parties, or one of them with the express consent of the others, to request that the content of the agreement resulting from the mediation be in written form. The content of the said agreement will be enforceable unless, in the present case, the content of this agreement is contrary to the law of the Member State where the request is made, or the law of that Member State does not establish its enforceability.[76]

2. The court or other competent authority may enforce the content of the agreement in a judgment or decision or in an authentic instrument in

[75] EU Press Release Reference: Mediation in civil and commercial matters, MEMO/08/263, Brussels, 23/04/2008,*available at* uropa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/2638rtype= HTML&aged=08dangiiage=EN&guiLanguage=en (last visited on 11 March 2020)

[76] Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* 166 (Cambridge University Press2010).

accordance with the legislation of the Member State in which the request is created.[77]

The researcher's view on this point is that it will be very difficult to have an international standard on the enforceability of agreements resulting from mediation (known as mediation settlement) because of the difference in culture, society and value of mediation in across different nations, particularly, between western countries and Asian countries.

6.7. India and ODR

There might be certain legal concerns regarding the implementation of ODR in India. For instance, if through a Delhi-based ODR institution, arbitration takes place while the arbitrator is in place in Mumbai and one part is in Chennai and the other in Bangalore, some legal issues are bound to arise. Foremost is the legal sanctity of such a system itself. Then arises the question of legal sanctity of proceedings, of e-mails exchanged, of documents and written submissions sent through e-mail, of the award rendered which is to be written and signed and lastly, the court which will have the jurisdiction to enforce the award.[78]

For this purpose, it needs to notice the Indian Arbitration and Conciliation Act, 1996 (Arbitration Act) with the Information and Technology Act, 2000 (IT Act). Some of the relevant issues are stated hereinbelow:[79]

(i) The Arbitration Agreement Shall be in Writing

Section 7(3) of the Arbitration Act provides that the arbitration agreement shall be in writing. But, if the parties agree online to transfer the matter to online arbitration through an ODR service provider, the question arises whether such an online agreement through an ODR service provider is valid, presuming that both parties admit that such an online agreement was

---

[77] *Id.* at 76.
[78] S.K. Verma And Raman Mittal (eds.) *Legal Dimensions of Cyberspace*, 320 (Indian Law Institute, New Delhi, 2004)
[79] *Ibid*

made, it will have the sanction of law due to the operation of section 4 of the IT Act.[80] When reading section 4 of the IT Act with sub-section 7(3) of the Arbitration Act, such an online agreement will be valid in the eyes of the law. The same applies to written comments, if any, made by online parties**.**

(ii) Award To Be in Writing and Signed:

Section 31(1) of the Arbitration Act requires the arbitral award to be in writing and signed by the member of the by the members of the arbitral tribunal. In such a case, an electronic award would have the same legal character as the offline award. Regarding the “writing” requirement, this is fulfilled in section 4 under the IT Act. As regards the signature requirement, section 5 of the IT Act provides that digital signature would have the same legal effect as a paper signature[81].

(iii) Applicability of the Electronic Award:

Another concern related to ODR is the enforceability of the obtained online award. The necessary question is that which court should a party approach to enforce an award? It will be the court of the place where the arbitration agreement was signed or will it be the court of the place where the arbitrators were sitting? Or will it be the court of the place where the award was issued? Or where is the ODR institution physically established? Or where are the parties established?

The answer is in the Arbitration Law itself. Section 36 stipulates that the award will be executed under the Civil Procedure Code, 1908 as if it were a

---

[80] Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference.

[81] Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then ,notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information of matter is authenticated by means of digital signature affixed in such manner as may be prescribed by central government.

court order. Section 2(e) of the law, "court" means the main civil court jurisdiction of origin in a district, and includes the High Court in the exercise of its ordinary civil jurisdiction, having jurisdiction to decide on arbitration matters if the same thing had gone to trial. Therefore, the court in which the award will be executed depends on the subject of the arbitration and not at the place of the arbitrator sits or where it renders the award or where it is established.[82]

Legal questions can be sorted out by a conjoint reading of the Arbitration Act and the IT Act as it gives the answers to various legal questions pertaining to the issues with regards to ODR.

6.8. Internet Jurisdiction in India

The E-commerce industry in India is growing faster in comparison to any other country and therefore India is faced with a large number of issues peculiar to the aspect of jurisdiction vis-à-vis the internet. In this segment the researcher will focus on some important aspects and issues regarding internet jurisdiction. For determining the jurisdiction of the Court in a dispute between the contracting parties, it is necessary to know where the contract in question was concluded. The place of formation of the contract determines the jurisdiction of the court in India where the breach of contract gives rise to cause of action. It is a well-settled principle that contract concludes:

- **(a)** where a letter of acceptance is posted in case of postal communication and
- **(b)** where a letter of acceptance is received where instantaneous means of communication has been used.

Positively different from the above two rules, the IT Act lays down rules for the place of dispatch and receipt of electronic records which may not necessarily be the actual place of dispatch or receipt of the electronic record.

[82] *Id.* at 78

Furthermore, it is quite possible that a contract may be actually concluded at a place different from that where the electronic record is deemed to be received. The IT Act has laid down an objective test which is the place of a transaction of the originator or that of the addressee where an electronic record is deemed to have been posted or received as the case may be. The actual location of the computer resource is not a determining factor. In a given situation, the computer resource of the originator or addressee used for the dispatch or receipt of the electronic record may be located in a jurisdiction other than that in which the originator of the transaction or addressee has a place of business. Further, contracting parties may not be conscious of the location of the digital resource used for dispatch or receipt of the electronic record. To address this uncertainty, the precise test has been laid down which takes into account the pace of business, regardless of the location of the computer resource. However, contracting parties are free to accept a different rule.

As far as the criminal law is concerned, the position has been straightened by the IT Act, 2000 which says that if the impact of a particular act is felt in India, Indian courts will have jurisdiction, thereby endorsing the effect theory.

Looking from a contractual perspective, the law is contained in the Code of Civil Procedure (hereinafter CPC), which says that the jurisdiction lies where the cause of action, whether wholly or partly, arises. This principle would mean even if a part of cause of action has arisen within the precincts or the jurisdiction of an Indian court, the Indian court could exercise jurisdiction. Section 20 of CPC doesn’t talk about due process or minimum contact principles. So, under this theory mere Web site access could suffice for a court to assume jurisdiction. The moment a plaintiff shows that the website is accessible from India, he can show that a part of the cause of action has arisen here because Indian viewers are likely to view the website. Both the Copyright Act and the Trademarks Act say that the plaintiff can file a suit where he is located, he doesn’t need to bother about where the defendant is located. This means Indian courts have a very wide jurisdiction as far as the Internet is concerned.[83]

But as has been noted, the courts in India are, to a large extent, looking at something beyond mere access of a website. In *Tata Sons v. Ghassan Yacoub and others*[84] where the defendant, Ghassan Yacoub, was based in the USA and had registered the domain name Tatagroup.com. The defendant had registered the domain name with Network Solutions Incorporated, which is a registrar based in the USA. The Delhi High Court did not go extensively into the question of jurisdiction but made a statement to the effect that the Internet has transnational ramifications, which means it potentially impacts almost every jurisdiction where it is accessible and one will have to look at where it's impact is felt. Based on this reasoning, the High Court of Delhi granted an ex parte interim injunction against the defendants restraining them from using and transferring the infringing domain name Tatagroup.com. The court observed that the contention put forth by the plaintiff that in matters concerning Internet communications, which have trans-national ramifications, the result of the challenged transactions in India is an important factor for determining jurisdiction.[85]

In, *Himalayan Drug Company v. Sumit*,[86] the plaintiff, the Himalaya Drug Company, had on their website a huge database on Ayurvedic concepts and the whole range of products and herbs listing out the herbs in their Sanskrit and Latin names, their properties, the medicines it was used in, etc. alongwith graphical and pictorial representation. The complete database was specifically copied by the defendant who lived in Italy and pasted on the website called ayurveda.sumit.net. The only contact with the plaintiff's was the one stated on the website in the form of an e-mail address 'sumit@democrat.com'. So, the

[83] S.K. Verma And Raman Mittal *Legal Dimensions of Cyberspace*, 303 (Indian Law Institute, New Delhi, 2004)
[84] Unreported ex parte interim injunction order; Suit No. 1672/99 (Delhi High Court)
[85] Jurisdictional issues relating to e-commerce , *available at* www.thelawbrigade.com (last visited June 8, 2021)
[86] Himalayan Drug Company v. Sumit, Suit No. 1719 of 2000 (Delhi High Court).

plaintiff sued the defendant along with the Internet service provider, also an Italian entity, virtualice.net, which had actually sub leased the domain name and web space to the infringer. The court exercised jurisdiction in this case because it was a case of copyright violation and under section 62 of the Copyright Act, 1957, a suit can be filed at a place where the plaintiff in based. Moreover the Web site could be opened in Delhi and the damage could also be said to have occurred there. The fact that the defendants belonged to Italy did not desist the court from exercising jurisdiction.[87]

In the case of *India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc & Ors.*[88] The court applied the doctrine of effect test of the United States Court. The case is linked to the launch of the television channel 'INDIA TV' in March 2004. As for the plaintiff, the brand was adopted from 01.12.2002 and requested the registration of the same brand on 22.01.2004. The brand was published in 2006 without any objection at the time. While searching the Internet, the plaintiff discovered the website <indiatvlive.com>. The plaintiff brought legal proceedings against the defendant for having definitively detained the defendant for the use of the mark. The defendant questioned the jurisdiction of the court because he claimed to be an American entity, not a resident in India nor working for gain in India. Understanding the incompetence of the traditional jurisdiction rules due to territorial jurisdiction being outside India, the court referred to the jurisdiction rule of the US court. The Court's decision deals with the application of the sliding scale and the effect formula and stated as follows:

I am in agreement with the proposition that the mere fact that a website is accessible in a particular place may not itself be sufficient for the courts of that place to exercise personal jurisdiction over the owners of the website. However, where the website is not merely 'passive' but is interactive permitting the browsers to not only access the contents thereof but also

---

[87] Dispute Resolution in Cyberspace: Determining Jurisdiction and Applicable Law, *available at* http://webcache.googleusercontent.com (last visited June 8, 2021)
[88] 2007(35) PTC 177 (Del.).

subscribe to the services provided by the owners/operators, the position would be different. However, as noticed in the judgment in CyberSell Inc. case , even where a website is interactive, the level of interactivity would be relevant and limited interactivity may also not be sufficient for a court to exercise jurisdiction. In Panavision International LP case, it was found that the registration of the Plaintiff's mark as a domain name by the Defendant had the effect of injuring the Plaintiff in California and therefore the court had jurisdiction. In CompuServe case again it was found that the defendant had contacted Ohio to sell his computer software's on the Plaintiff's Ohio based systems and sent his goods to Ohio further for their ultimate sale and thus those courts had jurisdiction.

In the present case, the website 'indiatvlive.com' of Defendant No. 1 is not wholly of a 'passive' character. It has a specific section for subscription to its services and the options (provided on the website itself) for the countries whose residents can subscribe to the services including India. The services provided by Defendant No. 1 can thus be subscribed to and availed of in Delhi (India) i.e. within the jurisdiction of this court."

The court held that since the website is accessible in India and the services provided can be availed in India, there are fair chances that the plaintiff may suffer economically. The court applied the effect test and finally held that the defendant is carrying on activities within the jurisdiction of this court and has sufficient contacts with the jurisdiction of the court.[89]

The e-commerce transaction has no national or international boundaries and is not parallel to the three-dimensional world in which Common Law principles were developed. From the advent of the internet, the issue of jurisdiction has continued to challenge the legal system, societies and country in the context of the peculiarly inherent character of the internet and thus diverse principles were evolved in different national jurisdictions in this regard.

---

[89] *Available* at https://epgp.inflibnet.ac.in/Home/ViewSubject?catid=20 (last visited on March 27, 2020)

Applications of e-commerce in the digital world limitless and the jurisdictional issues spawned by it are many and diverse. However, it is not the end. Once e-commerce applications of the internet are unfolded to its potential, jurisdictional issues likely to emerge may not be enforceable at present. It is quite possible that the supplier and consumer may be residing in two different nations. The questions which are likely to arise are: which nation has the jurisdiction in case of a dispute? Whether the laws of the nation in which consumer resides or the laws of the country in which supplier resides will apply? How to enforce the judgment?

Given the entire issue of jurisdiction from the Indian point of view, there is no established principle at this time. Article 19 of the Code of Civil Procedure is a provision from the Indian context which clarifies the situation in the case of multiple jurisdictions at the national level.[90]

Section 19 establishes that when a claim for compensation for a wrong done to the person or for a movable fact to the person or for a movable fact done to the person or to a movable property if the damage was done within the local limits of the jurisdiction of a court and the definition resides, or conducts business, or works personally for profit, within the local limits of jurisdiction of another court, the claim may be instituted at the option of the plaintiff in any of the said courts.

There is nothing wrong with applying the above principle to Internet contracts. As already discussed, jurisdictional problems in India are determined by the place of residence, the place of business or the cause of the action. The first is objective and easy to determine. The "cause of action" poses a serious problem in electronic commerce disputes. The jurisdiction of the cause of action is subjective and is probably debated in e-commerce cases.[91]

The IT law as amended in 2008 enacted in India fully complies with the UNCITRAL Model Law, but there is no reference to e-

[90] Online Dispute Resolution for Consumer, *available at* www.econstor.eu (last visited on June 8, 2021)
[91] *Ibid*

commerce. The entire IT Law was passed taking into account computer crimes. The legislators, when they were adopted, did not consider electronic commerce as an important aspect. Sections 11 to 13 deal in a limited manner with the sending and receiving of electronic documents, which apply to contracts. As such, there is no specific chapter in the IT Act that establishes the law related to e-commerce. The UNCITRAL Model Law is valid for developed countries. Since India is a developing country, the UNCITRAL model law does not meet its needs.[92]

The Consumer Protection Act, 2019 gives an additional advantage to consumers by providing the filing of complaints when the plaintiff resides or works personally for a lucrative profit. This would help eliminate the difficulties consumers face in seeking redress for their complaints against companies that may not have an office or branch in their state.

6.9. Conclusion

After having a discussion in regard to jurisdiction issues in e-commerce, it is notable that the internet jurisdiction is a subject of internal law and the basis of international to the nations conscience. Every country has its own laws and policy so a basic question that is any national law be enforced in the territory of the other nation is relevant. It is very clear that without any agreement or convention, no state can say to enforce its courts' judgment in another national court. The nation is bound by an agreement between two states or one state and two or more states. As discussed in this chapter, in USA judicial decision will prevail while in European Union statutory provisions will decide the jurisdiction. In Zippo case of American federal court clarified that once a website is sufficiently commercial and interactive beyond an entrance set by a court, jurisdiction may be established with every state. In Yahoo! case, US court denied to enforce French court decision and told the High Court of

[92] Uncitral model law - uncitral explanation, *available at* www.faculty.smu.edu (last visited on June 8, 2021)

Paris that its decision is not recognizable or enforceable in the United States because it violates the first amendment to the United States Constitution.

Indian has faced any case such as the Zippo or Yahoo case, thus there is no case law available on internet jurisdiction. Some high courts of India decide the case relating to cyber crime and cyber tort. But all cases are not directly related to e-commerce.

IT Act and newly enacted Consumer Protection Act 2019 describes internet crime and e-commerce in regards to consumer protection but these acts are silent on internet jurisdiction matters. The Information Technology Act intends to give legal recognition to e-commerce and e-governance and facilitate its development as an alternate to paper based traditional methods. The Act seeks to protect this advancement in technology by defining crimes, prescribing punishments, laying down procedures for investigation and forming regulatory authorities. Many electronic crimes have been bought within the definition of traditional crimes too by means of amendment to the Indian Penal Code, 1860. The Evidence Act, 1872 and the Banker's Book Evidence Act, 1891 too have been suitably amended in order to facilitate collection and admissibility of evidence in fighting electronic crimes. However, there is a lack of proper legal framework available to handle consumer protection and related issues. These inadequacies are apparent in IT Act and such relevant legislations and are unable to resolve e-commerce related issues.[93]

ODR in India is a very new concept. Government and private organizations give preference ODR regarding e-commerce dispute. It will be very helpful for online consumers who are in trouble when any dispute arises. ODR can be a feasible and positive step towards dispute resolution. Initial hurdles might arise, thus it requires to plan out a stage-wise development of ODR. The companies should take the lead by introducing in-house ODR facilities to enhance consumer satisfaction. It will take a while before the courts become tech-savvy and accept online awards for enforcement.

---

[93] S.K. Verma And Raman Mittal *Legal Dimensions of Cyberspace*, 232 (Indian Law Institute, New Delhi, 2004).

CHAPTER-7

CONCLUSION AND SUGGESTIONS

CHAPTER-7

CONCLUSION AND SUGGESTIONS

7.1 INTRODUCTION

This thesis has been devoted to the study of e-commerce and consumer protection strategy of e-commerce and comparing and projecting this against certain selected laws and policy. The thesis has been presented in seven chapters. The first three chapters (chapter 1, 2 and 3) set the stage by defining and explaining e-commerce, presenting the important issues of consumers and relating these to the study of different ICT tools and the status of e-commerce in the context of the growing digital divide. The chapter 4, 5, and 6 of the thesis is devoted to discussing and detailing international and national frameworks of e-commerce and the study of different internet jurisdiction issues. Final chapter of the thesis suggests important security measures to consumers in e-commerce and further suggests some reform in law regarding e-commerce issues like privacy, data protection, cyber fraud and misleading advertisement.

The current scenario of the Internet has presented various advantages to mankind of all ages, with the advancement in technology. One can easily assume how the internet has changed human life and has proved that "*change is the rule of life and the earth is round*". The internet has the same nature, it has connected the world unlike ever before. Today, anyone can watch each and everything at their own comfort with a single click and within seconds. The development of the country and the status of the people in a market was decided by society. However, the interne has revolutionized these aspects and changed the entire working and approach of consumers. No longer is one to think about his dressing or feel hesitant in entering a branded store for he no longer needs to enter a market or shop physically, all he needs to do is to access the internet and enjoy the ease of e-commerce by a single click. E-commerce has changed the way of thinking and of doing business. It is a green economy, paperless and eco-friendly.

E-commerce is a part of the information technology revolution and it has been widely used in global commerce in general and especially in the Indian economy. In the last few years, it has seen a technological revolution brought about by the widespread use of the Internet, digital technologies and their applications.

As a result of globalization, e-commerce represents the forefront of success in the digital age and has changed and continues to change the way business is done around the world. The commercialization of Internet technology has made e-commerce one of the smartest channels for inter-organizational business processes.

Although business-to-business transactions play an important role in the e-commerce market, business transactions with consumers generate a large share of e-commerce revenue in rapidly developing countries like India. Electronic commerce has multiple benefits for consumers in the form of availability of goods and services and is also time saving. An individual can purchase products with the single click of a mouse without leaving their home or office. In addition, online services such as banking, ticketing (including airlines, buses, and railways), bill payment, hotel reservations, etc. have been of great benefit to customers. Internet companies like financial services, travel, entertainment, and supermarkets are likely to grow fast.

In e-commerce the consumers can defend themselves against undesirable terms more easily in the electronic environment. E-consumers can shop in the privacy of their homes, where they can make thoughtful decisions without time constraints. They can drop their computers and return before making their transactions, giving them time to think and investigate further. Also, at present, e-consumers tend to be better educated and wealthier than paper-world consumers, suggesting that they can better fend for themselves in the marketplace.

7.1.1 Corona Virus: E-commerce Gets a Boost as Consumers Prefer to Stay Indoor

The spread of corona virus (COVID-19) cases in India has had some influence on the food collection and ordering sections, it has become an advantage for e-commerce companies as more and more people prefer to buy goods and services, especially food, vegetables and other daily needs from digital platforms. According to the e-commerce industry, in such a circumstance, where a growing number of people are also working from home, these firms are doubling down to bring convenience to the consumer and gain their trust. There was a 25% spurt in online shopping grew in February 2020 due to fear of coronavirus. This has put extra pressure on the delivery system. IT companies like TCS, Infosys as well as the education sector are working from their home. These companies are seeing a high demand for products and services such as fresh fruits and vegetables, milk, flour, rice, and lentils, and personal hygiene items like sanitizers and soaps and household cleaning products. Other products include baby food, instant noodles, and Ayurvedic items. [1]

Snapdeal, an e-commerce company supported by SoftBank, said overall orders are still strong, with some categories experiencing rapid growth. Sales of masks and toiletries such as disinfectants and hand washes have increased 25 times in Snapdeal over the last five days. Over 50% of the masks sold at Snapdeal were sold on the day India reported the first suspected COVID-19 case.[2] The coronavirus has provided a golden opportunity for the e-commerce industry to increase customer confidence, as orders on platforms like Amazon, Flipkart and Bigbasket become a lifeline for them. Suppose there is a deadlock

[1]Corona Virus: E-commerce Gets a Boost as Consumers Prefer to Stay Indoor, *available* at https://www.business-standard.com/article/companies/coronavirus-e-commerce-gets-a-boost-as-customers-prefer-to-stay-indoor-120031500022_1.html) (last visited on March 12,2020)
[2] *Ibid*

due to COVID-19, e-commerce companies are more than willing to partner with government and safely provide essential products to people.[3]

According to industry insiders, e-commerce companies such as Flipkart, Amazon, Bigbasket and Grofers have seen orders increasing by around 20-30% as customers avoid visiting crowded places like malls and supermarkets.

The growth in e-commerce was driven by rapid technology adoption that was led by the increasing use of devices such as smart phones and tablets, and access to the internet through broadband, 3G, 4G and now 5G, which led to an increased online consumer base. Moreover, it favoured demographics and a growing internet user base helped and aided this growth. In terms of highlights, the growth shown by home ground players such as Flipkart, Snapdeal, etc and the interest shown by large multinational corporations such as Walmart, E-bay, Alibaba, etc., reflects the growth of the company and displayed the immense potential of the market.

Following data shows that how e-commerce diverted the life of every human being and the position of the consumer in the newly booming e-commerce market system in India:

1. E-commerce has transformed the way of doing business in India. The Indian e-commerce market is expected to reach $ 200 billion by 2026, up from $ 38.5 billion in 2017. Much of the growth in the industry has been triggered by increased penetration of the Internet and smartphones.[4]
2. The ongoing digital transformation in the country is expected to increase the total Internet user base to 829 million by 2021, up from 636.73 million in fiscal 2019. India's Internet economy is expected to double from US $ 125 billion in April 2017 to $ 250 billion by 2020, largely due to e-commerce. India's e-commerce revenue is projected to

[3] *Id.* at 1.
[4] E-commerce in India: Industry Overview, Market Size, *available* at https://www.ibef.org/industry /ecommerce.aspx (last visited on March 12,2020)

grow from $ 39 billion in 2017 to $ 120 billion in 2020, with an annual growth of 51%, the highest in the world.[5]

3. Driven by the growing penetration of smartphones, the launch of 4G networks, and increasing consumer wealth, the Indian e-commerce market is expected to reach $ 200 billion by 2026, compared to $ 38.5 billion in 2017. 31% to reach $ 32.70 billion in 2018, led by Flipkart, Amazon India, and Paytm Mall.[6]
4. Between April and June 2019, smartphone shipments to India increased by 9.9% year-over-year to 36.9 million shipments. It is expected to reach 160 million in 2019.[7]
5. In 2018, electronics is currently the top contributor to online retail sales in India with a 48% share, closely followed by apparel with 29%.[8]

Despite the above data, every coin has two sides one side is white and another black. E-commerce also has some black side. It has presented many difficulties to the traditional laws and the legal system throughout the world. The risk to consumer privacy, cyber fraud, card cloning, etc, lots of cases happened every year where the consumer was cheated by the companies, his account and personal sensitive data stolen by cyber thieves. A large number of data is now available that shows that the ration of cyber fraud, consumer cheating, and violation of cyber privacy, etc., is growing fast every year. Some data of NCRBC are as follows: [9]

1. As per the statistics of the National Crime Records Bureau (NCRBC) cybercrimes in India has almost doubled in 2017, the data comes in the backdrop of India aspiring to become a trillion-dollar digital economy. An interesting fact that cyber crimes evaluated less than a percentage

[5] *Id* at 1.
[6] Corona Virus: E-commerce Gets a Boost as Consumers Prefer to Stay Indoor, *available* at https://www.business-standard.com/article/companies/coronavirus-e-commerce-gets-a-boost-as-customers-prefer-to-stay-indoor-120031500022_1.html) (last visited on March 12,2020)
[7] *Ibid*
[8] *Ibid*
[9] Cyber crime cases in India almost doubled in 2017, *available* at https://www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017 11571735243602.html (last visited on March 11,2020)

(0.43%) or 21,796 cases out of a total of 50.07,044 recognizable crimes in 2017.

2. As per the statistics of NCRBC, during 2017, 56.0% of cyber-crime cases registered were for the motive of fraud (12,213 out of 21,796 cases) followed by sexual exploitation with 6.7% (1,460 cases) and causing dishonor with 4.6% (1,002 cases).
3. Centre trying to fortify India's cyber operations amid rising warnings of malware attacks on personal and organizational devices, cyber law experts and intelligence have stated much like crimes against women, India suffers from dismal under-reporting of cybercrimes.
4. India registered 9,622, 11,592 and 12,317 cases of cybercrime in 2014, 2015 and 2016 respectively. The data for 2017 released after a two-year long wait, with the Centre blaming states for the delay in providing statistics for compilation.

The data has now been collected in more detail for various categories of crime. For example, under cybercrimes against women and children, NCRB crime statistics states that lots of cybercrime such as cyber blackmail, cyber pornography, cyber harassment, defamation, molestation, fake profile, internet crimes through other games rapidly growing in e-commerce transactions.

As per the information reported to and tracked by CERT (Indian Computer Emergency Response Team) in the number of cyber security incidents in India was 50,362 in 2016, 53,117 in 2017 and 2, 08,456 in 2018. The figure had touched the number 3, 13, 649 by October 2019. As per the logs analysed, the Internet Protocol (IP) addresses of the computers from where the cyber attacks develop to have started belong to various countries, including India, North Korea, Pakistan, Algeria, Brazil, China, France, Russia, Serbia, South Korea, Taiwan, Thailand, Tunisia, the USA, the Netherlands, and Vietnam. Cyberspace knows no borders, physical or virtual.[10]

[10] Cyber crime net widens ,*available* at https://www.tribuneindia.com/news/cyber-crime-net-widens-21638 (last visited on March 11,2020)

In the researcher's view, Cyberspace has inherent vulnerabilities that simply cannot be done away with. There are countless entry points on the Internet and technology makes it relatively easy to divert allocation to other parties. E-commerce needs no boundary so countries-states, non-state operators, such as terrorist organizations and criminal gangs, as well as individuals, are capable of carrying out attacks at different levels, targeting government networks, companies and financial systems. or solitary persons and an individual as well as a consumer from small cites and people from rural areas are targeted rapidly for financial fraud or to hack personal information.

One of the major tasks before e-commerce at the global level is to find a correct harmony between the laws of two nations and the enforcement of judgment in other nations territory. The question arises whether, in light of current technology, it is possible to do business over the Internet in one jurisdiction but not in another. If a company provides a link on its website through which a person in one country can do business with the firm, is it technically possible for that the company to block access to someone in other nations?

Keeping in mind the flaws of the present law and policies regarding the above issue, this concluding chapter of the thesis briefs out the conclusion of the research and suggestions for a different strategy for dealing with e-commerce and consumer protection issues.

7.2 Summation

Every breath you take and every smile you fake

Every move you make and every step you take

Every claim you stake and every vow you break

I'll be watching you

Every single day, every word you say

Every game you play, every night you stay

I'll be watching you[11]

These words expressed in an iconic song reflecting the emotions of a disgruntled lover**,** befit the situation that persists with the Internet.

This thesis has shown a sharp contrast between faltering protection of consumers' critical interests and protection in e-commerce on the one hand, and legal framework of e-commerce and optional dispute resolution. In the course of the research work, the researcher has come to the finding that the term 'electronic commerce' refers to all forms of business and commercial transactions that are carried out through and over a digital medium. It has been defined as a new way of doing business that is transforming trade and commercial relationships across the globalised world. Countries, particularly India, need to understand and participate in this new phenomenon and create an environment conducive to its development in their own economies. To do this, they must have in place the right law and policy and strategy regarding e-commerce and consumer protection that prepares their economy for e-commerce opportunities.

This research has shown that in view of the growing importance of e-commerce for economic growth in developing countries like India which face a special challenge and responsibility to create a conducive policy environment that on the one hand allows for the development of e-commerce and on the other ensures the social objective of providing access and benefits for those that cannot afford it.

Chapter 2 of this thesis has described research activities aimed to investigate how e-commerce developed from the advent of internet to modern digital market perspective in order to various ICT tools that played a vital role for the development of e-commerce and consumer acceptance of this digital market. The research has explored different spectrums like 3G, 4G and 5G with

[11]The police every breath you take lyrics , *available at* https://genius.com/The-police-every-breath-you-take-lyrics , (last visited on March15, 2020.)

the help of recent statics. This research has taken into account various factors that determine (in brief) consumer acceptance of digital method of payment systems, such as usability, privacy, security, trust and others.

The cyberspace comes with many inherent dangers towards technology like privacy issue, cyber negligence, cyber crime etc. The internet is the greatest structure of human beings in history, it originated new ways of consumerism and changed the meaning of consumer is king. Today's consumer who is now an e-consumer, seller changed into e-seller, market changed into e-commerce, has changed the entire concept of market and society. Chapter 3 of the thesis tested the whole consumer mechanism of e-commerce and it has also included in detail various torts and crime that was done by the digital medium. The cyberspace comes with inherent dangers to privacy. Though the concept of privacy protection is old. Creative interpretation of law is required to deal with new tools for tracking and stalking people on the information superhighway.

Consumer rights are part of the basic rights of a human beings, as it protects them from the wrongdoings of companies and selling their products. It empowers the individual to fight for his rights as a consumer, to fight against the fake promises made by companies and sellers to sell their products and services, and most importantly consumer rights serve as a legal weapon against the injustices of companies and business organisation.[12]

Creating new technologies is the job of inventors. Using these technologies for more advanced and more radical crimes is the skill of cyber criminals. Controlling such crimes is the result of the interplay of the functions of the legislature, executive and judiciary. It is a circle. The society rubs in between this circle with different emotions and reactions. Sometimes, with fear as a new invention springs up, then with distrust when the invention is used for anti-social activities and then with hope as the Big Brother nails down the criminals with the shackles of law. This is how the telegraph was looked at; the Internet is being viewed in this way. This is how future technologies will be

[12]World consumer rights day, *available* at https://www.mapsofindia.com/my-india/government/world-consumer-rights-day (last visited on March15, 2020.)

looked at. However, the time frame between each activity is tremendous. In between certain situations, the wrongdoer or computer criminal are able to gain the maximum. However, as the wheels of judgment become operational with just oiling of the law and evidence, such unsociable activities are forced to reduce. Though, on a cautious note, they never tend to cease.[13]

Information Communication Technology (ICT) has opened up a lot of opportunities for countries and people. Today, ICT presents the lowest means of conducting e-commerce transactions via the Internet. Buying and selling through the Internet otherwise called electronic commerce (e-commerce), is fast-growing around the globe. Every day, millions of online transactions involving millions of US Dollars take place on the Internet. In fact, this advancement has led to the current legal measures becoming outdated**.** Chapter 4 of the thesis has focused on the international legal framework of e-commerce and it may be noted that when we talk about international law of e-commerce United Nation always try to has provided substantial laws for universal application with regards to e-commerce. In this regard, the UN has passed Model laws in 1996 on electronic commerce also known as the UNCITRAL Model law.

In 2005, United Nations had adopted a Convention on the Use of Electronic Communications in International Contracts. It was adopted in November 2005 and entered into force on March 1, 2013. It aims to facilitate the use of electronic communications in international trade by ensuring that contracts concluded and other communications exchanged electronically are also valid and applicable with respect to their traditional paper equivalents. It intended to strengthen the harmonization of e-commerce rules and promote uniformity in the national promulgation of the UNCITRAL model laws relating to e-commerce, as well as to update and integrate certain provisions of those model laws in light of recent practice.[14]

[13] Devashish Bharuka, "Indian Information Technology Act, 2000: Criminal ' Prosecution Made Easy for Cyber Psychos", 44 *JILI* 354 (2002).

[14] Dr. Vivek Kumar, “An study of E-commerce and its legal frame work: With special reference to India’’ 89-94 *International Journal of Law* 3; Issue 3; (May 2017)

Organisation for Economic Co-operation and Development (OECD), The Hague Conference, 1995, WTO working Programme on E-Commerce, Anti-cyber Squatting Consumer Protection Act, 1999 have been taken for discussion in Chapter 4. The various UN laws have played a significant role in order to harmonise law on e-commerce but due to conflicts between the interests of various countries such as the developed and developing nations, there still persist significant differences. Every country has their own interest on commercial issues, thus any WTO meeting or any UN conference on this issue always failed to reach on universal agreement and this resulted in the problem of faced by consumers who have suffered on this account in international companies and markets.

Chapter 4 of the thesis has carried out a study on international law relating to e-commerce and consumer protection. It is well settled that e-commerce contributes immensely to the global economy. E-commerce can encourage the economy of any country. In so far as that country wishes to take the advantages brought by the breakthrough in the modern-day information technology. However, it is not possible to achieve without putting in place the relevant legal framework that will protect online consumers or e-consumers.

The Indian framework of e-commerce has been discussed in chapter-5 with the increasing use of information and communication technologies (ICT), a new branch of jurisprudence known as cyber law or cyber space law or information technology law or internet law emerged to regulate law and order in cyberspace. In 1996, for the first time, a Model Law on Electronic Commerce (MLEC) has been adopted by the United Nations Commission International Trade and International Law (UNCITRAL), which was later adopted by the United Nations Assembly. The principal aim of MLEC was to bring a uniform law regarding electronic commerce at the international level and bringing electronic transactions to the level at par with paper transactions to determine the rights and obligations of the transaction parties similar to those of paper transactions. India is a signatory country to this model law promulgated the Information Technology Act 2000. Consequently, to give effect to UNCITRAL Electronic Signature Act (MLES), 2001 India promulgated Information Technology (Amendment) Law of 2008.[15]

The Indian government enacted the Information Technology Act 2000 (the Information Technology Act) in June 2000 in response to the need for legislation that legally recognizes transactions made electronically. The discovery of gaps in the law on the basis of a judicial review led the government to modify the said law in 2008 by introducing provisions concerning, among other things, the validity of electronic contracts, the security of electronic signatures, the sanctions for computer crimes, identity theft, breach of privacy and publication and transmission of obscene material in electronic form. With the advent of growth in the IT sector, particularly the increased role of Internet Service Providers (ISPs) and payment intermediaries in India, the government has crystallized the role and responsibilities of the 'intermediaries' under IT Intermediary Rules, 2011 to sanctify IT safe haven provisions, to protect service providers against third-party data.[16]

However, there have been other cases where the government has come under heavy criticism. For example, there have been discussions about preselecting content, particularly on social media websites. The scope of objectionable content also appears to have been broadened to include criticism of the government.

IT Act is the main law that regulates Internet use in India. IT law regulates online conduct and related aspects of e-commerce and recognizes e-contracts, cybercrime, internet surveillance and intermediary liability. Special laws and policy, such as the Payment and Settlement Systems Act 2007, govern payment system operators and payment intermediaries, including in the e-commerce sector. Time to time, Reserve Bank of India (RBI) publishes guidelines governing the use of electronic payment instruments (e.g. gift cards,

---

[15]Raj, Aijaj & Rahman, Wazida, E-commerce Laws and Regulations in India: Issues and Challenges 44-51 *Researchgate.net* 1 (2016)

[16]Demystifying IT Rules 2011: What it means for you, *available* at https://nishithdesai.com (last visited on June 20, 2021)

electronic wallets, credit cards and debit cards) for facilitating e-commerce and mobile commerce. In March 2016, guidelines issued on foreign direct investment (FDI) in e-commerce, the Department of Industrial Policy and Promotion (DIPP), Ministry of Commerce and Industry of the government of India. , which were afterward replaced and revised by the Press Note of December 2018 issued by the DIPP in December 2018. The introduction of Press note is an important development as it provides transparency to the existing FDI framework concerning the e-commerce sector.[17]

In 2019, The RBI has amended the Foreign Exchange Management (Transfer or Issue of Security by a Person Resident outside India) (Amendment) Regulations 2019 dated 1 February 2019 to make it consistent with the amended legal framework stipulated under Press Note 2018. The RBI Regulation, 2019 may play a vital role and may become the backbone of the legal framework within which business maybe conducted via the internet in India.

According to the IT Act, 2000 the provisions under the Indian Evidence Act, 1872, the Indian Panel Code, 1860, Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 pertaining to e-commerce were also amended to address the concerned issues of cybercrimes and evidence, and to enable additional regulation as regards electronic fund transfer. [18]

In the view of the researcher, the main problem generally faced by developing economies like India is that with a completely different economic as well as technological set up, the proper and a replica implementation of such 'high-tech' legislations as envisaged by the Model laws becomes very difficult. Even if the legislature fulfils its obligation by enacting a law, it becomes difficult to enforce and implement it in the Indian scenario. Thus, a critical analysis of the existing laws and regulations shows that various legal issues such as jurisdiction, taxation, data privacy in e-commerce remain untouched. The country requires effective law and regulations for making e-commerce

[17]https://gettingthedealthrough.com/area/11/jurisdiction/13/e-commerce-india/(last visitedMarch18,2020)
[18]https://www.researchgate.net/publication/330845555_Ecommerce_Laws_and_Regulations_in_India_ Issues_ and_Challenges (last visited March18,2020)

transactions fairer and achieving a more consumer-friendly e-commerce environment in India.[19]

The core elements of e-commerce are registering the order, arranging the delivery, and receiving e-payments. If and when such problems arise in such transactions, the setback can be irreversible and are to be addressed with expediency. The settlement of disputes in the B2C segment, particularly, is challenging. Disputes are traditionally located within the physical territory where one or both of the disputants are located. Different principles are applied in different national jurisdictions in this regard. In the beginning, courts in different countries began to access the internet merely to use it as a sufficient ground for assuming jurisdiction over internet related transactions.[20] Jurisdiction dispute in e-commerce has been taken up in Chapter-6. The Chapter takes up the USA, European Union, Hague Convention 2005 on Choice of Court with detailed discussion on leading case laws on Yahoo case in European Union and Zippo case in USA. USA court applied two types of theory to resolve jurisdiction dispute:

I. General jurisdiction
II. Specific jurisdiction

General jurisdiction is asserted over a non-resident defendant only if the defendant's contacts with the state are "continuous and systematic", even if the contacts are unrelated to the dispute at hand.[21] Specific jurisdiction arises when the lawsuit is related to the defendant's contacts with the forum state.

The U.S. courts underlined the fact that orders of a foreign court against a legal entity of another country would not automatically become operable in

---

[19] *Id at* 17
[20] M.M.K. Sardana, "Evolution of E- Commerce in India: Challenges Ahead (Part 2)" 3 *available* at: http://www.isid.org.in/pdf/DN1408.pdf (last Visited on Marche 18, 2020).
[21] *Specht* v. *Netscape Communications Corp.,* 150 F. Supp. 2d 585 (SDNY 2001) affd,306 F.3d 17 (2d Cir. 2002).

the country of origin, but would need scrutiny by the court of the country of origin with reference to its laws and constitution.[22]

Courts have established the benchmark for determining jurisdiction based on the level of interactivity and the commercial nature of the exchange of information that occurs on the website in a particular jurisdiction and have classified website activities in three areas:

a) Fully interactive sites where users buy goods or services, exchange information or files, or enter into agreements;

b) Completely passive sites where the information is available for people to see;

c) Websites somewhere in the middle, with restricted interaction.

Courts are likely to take jurisdiction over the out-of-state operator of fully interactive sites, unless the operator forbade the sale in the state or did not target them. Fully passive websites are not likely to be subject to jurisdiction as they operate from outside the state.[23]

Online Dispute Resolution (ODR) like arbitrator and mediation are new tools in e-commerce issue regarding cyber jurisdiction. Part 2 of Chapter 6 deals with ODR. The concept of ODR has emerged in various jurisdictions due to globalization. The many benefits of ODR include less time, speed, costs and convenience. These advantages make it more lucrative than traditional methods such as litigation. Due to inadequate e-commerce laws, lengthy litigation process and overcrowded Indian courts, ODR is a more convenient way to handle e-commerce litigation in the world, including consumer complaints.[24]

[22] Abha Chauhan, "Evolution and Development of Cyber Law - A Study with Special Reference to India," *available* at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2195557 (last Visited on Marche 18, 2020).

[23] https://www.researchgate.net/publication/330845555_Ecommerce_Laws_and_Regulations_in_India_Issues_and_Challenges (last visited March18,2020)

[24] http://legalreferee.com/odr-e-commerce-india/ (last visited March18,2020)

Indian laws on cyber jurisdiction are unable to deal with e-commerce disputes, the issues relating to jurisdiction and enforcement in e-commerce is still remain in their nascent stage in India. In general, a number of local statutes provide for a 'long-arm jurisdiction' whereby the operation of such local laws have extra-territorial application if an act or omission has resulted in some unlawful or prejudicial impact within the territory of the country. The IT Act vide Section 75 has been extended to the whole of India and will also apply to any contravention there under committed outside India by any person and the law applies to any crime or offense committed outside India by any person if the act or behavior creating the crime or violation involves a computer, mobile, smart device, computer system or computer network located in India.[25]

Section 3 of the Indian Penal Code (IPC), 1860 provides that any person who is liable, by any Indian law, to be tried for an offence committed beyond India shall be treated under the provisions of the IPC for any act committed outside India in the same way as such an act was committed in India. Therefore, there does not seem to be too much jurisprudence in India on the issue of jurisdiction in electronic commerce cases.

India has not had any case law like Zippo and Yahoo, thus there is no case law available on internet jurisdiction. Some high courts of India have decided cases pertaining to cyber crime and cyber tort. But all cases are not directly related to e-commerce. Due to the borderless nature of the Internet, "territorial" jurisdiction becomes complex. Furthermore, regarding various categories of disputes, issues such as jurisdiction, choice of law and the high cost of cross-jurisdiction litigation may arise. There are certain loopholes in the IT Act such as ambiguity with respect to the legal jurisdiction of contracts involving international parties and absence of dual-key pairs for individuals and business, compromising the confidentiality of e-transactions.

[25]The extra territorial jurisdiction of the Indian criminal courts, *available* at http://www.shareyouressays.com/knowledge/the-extra-territorial-jurisdiction-of-the-indian-criminal-courts/115819 (last visited March18, 2020)

A developing nation, including India, must strive to draft a comprehensive e-commerce law, which inter alia also addresses issues pertaining to consumer disputes and cyber jurisdiction issues. the nature of e-commerce is too technical that the present law and policy are unable to deal with the e-commerce situation. The entire discussion shows that e-commerce law remains as the foundation and serves as a last resort to resolve e-commerce and consumer disputes. Courts, however, need to consider policy implications because the Internet is a new medium of communication that forces e-commerce law to evolve. Further, the significant approach that e-commerce requires all the formalities of traditional laws but at the same time, commerce has drastically changed on account of e-commerce, technology, internet. Thus, the present legal infrastructure may not be best suited as a remedy for consumer rights infringement in cyberspace. Of course, the basis of traditional law should not be lost while drafting specific provisions, rules, and regulations pertaining to e-commerce law and policy. However, the technical aspects must be given due weight and appropriate treatment while framing the relevant provisions in Cyberspace commerce.

Recently India enacted the new Consumer Protection Act, 2019 which includes e-commerce and misleading advertisement but this Act does not provide an adequate remedy to the e-consumer victim. The government of India launched the Digital India program, which is a program to transform India into a digital society and a knowledge economy. Digital India is transformative and would ensure that government services are digitally accessible to citizens. It would also allow public accountability through the mandatory provision of government services electronically, a unique identifier and an e-Pramaan based on authentic, interoperable and integrated standards-based government data and applications. It provides a safe and secure cyber environment.

Despite of Digital India program and law, consumer awareness is a significant problem in India. With the advancement and popularity of technology, recent cases of cyber crime in India have also increased. Today, several cyber crimes like kidnapping, fraud, hacking, and data theft are being committed with the help of the internet. Cyber Criminals and hackers targeted non-technical or less aware consumers easily through phone calls, emails, etc. every day the cyber crime and consumer fraud cases in India are registered under the IT Act.

Digitalization is uncontrolled these days and the Internet has made life easier for everybody, by everything just a click on the keyboard. The number of cyber crimes and consumer fraud cases in India has increased. It has made individuals dependent on technology for every little basic need. Now a days, the everyday requirements are also available 24 hours 7 days a week through online shopping, ordering food, making payments, etc.

To summarize the statement, it can be concluded that, despite the growing use and importance of the Internet, legal regulations do not yet fully cover the potential problems associated with cyberspace, nor provides adequate protection for electronic consumers. There is a need for greater efforts and suitable law to protect and create awareness amongst consumers and to protect their rights. In the USA, judicial precedent available for solving e-commerce disputes and in the Zippo case, the American court applied a personal jurisdiction test to protect consumer rights. In the European Union the legislation available on e-commerce dispute, Brussels-1 and Brussels-2 Convention provides adequate measurement to solve consumer disputes in e-commerce. In India, the situation is not good in regard to e-commerce, not a single case available on issue of e-commerce of the Supreme Court. Some High Courts have decided e-commerce cases but those cases have not had much impact on e-consumer protection.

On the basis of research work done in the thesis, hypothesis tested and resulted

1. Protection of consumer rights is a major concern in e-commerce.

The first hypothesis, protection of consumer rights is a major concern in e-commerce has been tested based on the most relevant aspects regarding this question. This aspect is that is protection of consumer rights is a major concern in e-commerce? Based on the analysis made under chapter 3 of this thesis following conclusions can be made with regard to this question:

- Commerce is global and transnational in nature, many efforts and policies have been made at the national and international level to ensure the protection to e–commerce. Despite of these, explaining e-commerce principle is a very difficult task at the international level because every nation has its own interest, own law so how can there be a universal formula.
- In India there is great diversity in consumers lives here, maximum consumers are not technically sound, some consumers are illiterate and some have knowledge of computers but are not up to date with the technological advancements. Every day a lot of cases of violation of consumer rights are happening and exploited by online shopping websites and consumer have no option to protect his right.

2. There is a lack of uniform standard to goods' quality, security and privacy. Multiple financial, organizational, technological, and managerial issues are not being addressed.

The boom in e-commerce has certainly changed the way we buy in a better way. But like everything else, the world of online shopping is not so bright. Despite all efforts by e-commerce companies to mitigate them, customers are facing certain problems with online shopping.

The quality of products and services is a big issue in online shopping. Reviews are not always reliable and all the research can't assure you of a product's quality; fake sellers who intentionally cheat customers to increase sales are the prime reason for faulty and bad products being sold online. The standard of the product is not the same in each country and due to the lack of proper law e-commerce, companies sell the same product but different standards. The problem of e-payments always appears overhead while making online transactions. A slow internet connection or a technical error often results in the payable amount being debited from a customer's account without being credited to the seller account. E-commerce sites record consumer sensitive data like name, address, income, and account. In lack of cyber security measure consumer data can be used by hackers.

The return of product and refund money is a big headache in online shopping. Due to a dissatisfied customer or damaged product, the consumer always face a lot of annoyance from e-commerce website's enquiry and policy. There is no physical contract between consumer and seller so need to reform financial, organizational, and managerial infrastructure by the e-commerce companies.

Thus the second hypothesis, There is a lack of uniform standard to goods' quality, security and privacy. Multiple financial, organizational, technological, and managerial issues are not being addressed has been tested and proved on the basis of analysis made under chapter 2 and 3.

3. There is lack of national and international government regulations and industry standards regarding e-commerce.

E-commerce laws are not similar or universally consistent and to regulate transnational commercial transactions over the Internet, the national laws and policies are not ready to face the issues pertaining to borderless environment of the Internet. The courts around the world also are unable to come up with a coherent doctrine of e-commerce law for Internet transactions.

Electronic commerce requires consistency in regulations. But the challenges that electronic commerce presents to regulators force them to change their minds on several occasions. Even in developed countries, like the United States, where there is a debate over the applicability of state taxes to e-commerce transactions, so one can imagine the inconsistency of legal and tax regulations in developing countries.

Every nation has its own set of rules that what does or don’ts about what can be sold to whom. Most countries consider transactions made by minors to be inapplicable, but the exact age of the legal age varies by country. Likewise, several categories of products -medicine, food, alcohol, weapons, etc, among others have specific requirements.

Some countries in the world have a relatively weak legal framework. Although some countries have a strong legal framework, the court process is often significantly delayed. For this reason, while an online retailer may have to comply with the laws of that country for all practical purposes, it may not be able to protect its legal rights in that country.

Another very important issue of cyber jurisdiction is in electronic commerce. The problem is to know which court is competent to hear a dispute between the parties resulting from an e-commerce transaction. In addition, what law should be applied by the said court? This is due to the fact that the parties may reside in different places with different legal systems.

If a country finds a person on its territory, it exercises its jurisdiction over this person. The Internet significantly reduces the importance of the parties' physical location, as transactions in cyberspace are not geographically based. In addition, the Internet is upsetting the balance of power between the distributor and the consumer, as consumers now have instant access to large amounts of information and highly sophisticated analysis tools. This affects the basis on which the courts have analyzed the ability of consumers to make binding decisions in law and in forums.

International law based on nation’s agreement so it is very clear that without any agreement or convention no state can say to enforce the judgment of its court on another national court. The nation is bound by an agreement between two states or one state and two or more states.

Therefore, the third hypothesis, is that there is lack of national and international government regulations and industry standards regarding e-commerce, has been validated in chapter 4, 5 and 6.

4. Advertising affects consumers' choices regarding what they buy and it is not legally addressed.

Advertisement always plays a significant role in the choice of consumer that what to buy and what not to buy. Consumers believe that if celebrities are saying in an advertisement that some products or services are good, surely that product or service will be good for health or life. In maximum cases of advertisement, consumers are cheated by the companies. Celebrities and companies mislead the consumer choice and inspire the consumer to buy a specific product through fake advertisement.

The worst aspect of fake and unethical advertising on consumers is perhaps, they change the situation of consumers; they buy a product without knowing their financial capacity and quality of the product. The consumer ends up making uninformed decisions. If the company doesn't tell its customers about the truth of the product or terms and conditions of services, the consumer will make poor decisions concerning those products and services. Consumers will end up wasting valuable money on something, which ultimately, really won't meet their needs or solve their problems; ultimately, the consumers use the product without knowing the negative side effects of the product and services.

The issue of misleading advertising is a complex problem in electronic commerce. Companies, by sending out misleading advertisements, which affect consumer decisions, are unfairly trying to convince consumers to believe in advertisers' ideas and thereby affect the other person's ability to compete.

Hence on the basis of the analysis in chapter 3, the fourth hypothesis advertising affects consumers' choices regarding what they buy and it is not legally addressed, has been proved and justified.

7.3 SUGGESTIONS

The question before us is how to design the most excellent e-commerce law and policy and how to protect consumer rights in e-commerce. To this end, some view suggests that the acceleration of technological change is so great that the legal system cannot keep pace. This view is offered in support of any number of propositions: e-commerce law should have a similar parameter in each reason because it is a transnational transaction. The legal system is nevertheless the mechanism through which disputes in modern society are decided. There should be a proper mechanism to protect e-consumer rights. Keeping in mind the flaws of the present policies regarding the above issue, the following recommendations are suggested:

7.3.1 Suggestion Regarding Law and Policy

- In India, strict implementation of legal provisions is the biggest problem, which provides opportunists to the cyber criminals to break and abuse the law. There is a need to create an active cyber cell, a national nodal agency[26] and a computer disaster response team[27] in each state which are empowered to meet the challenges and danger of the Internet. The Cyber Crime Investigation Unit is an essential wing of the Directorate of Crime, headed by an officer of the rank of DIG, assisted by several officers of the rank of Superintendent of Police, Deputy Superintendent of Police, Inspector and Sub-Inspector. The unit works under the overall control and supervision of the state DGP. For proper

[26] Section 70-A of the Information Technology Act, 2000 provides establishment and role of National Nodal Agency (Inserted vide ITAA 2008).

[27] Section 70- B of the Information Technology Act, 2000 states procedure of establishment and powers of the Indian Computer Emergency Response Team to serve as national agency for incident response. (Inserted vide ITAA 2008).

functioning of the cell, it has a number of sub-units such as testing units, cyber laboratories and police stations. The investigation unit consists of investigators from various ranks. According to the Information Technology Act, an officer not below the rank of the inspector can investigate cybercrimes. The cell has cyber labs to assist investigators in the investigation process. The lab has facilities for recovering deleted data, cell phone forensics and email tracking etc. There is a notified police station under this cell where an FIR can be registered in relation to cyber crimes. Despite adequate protective action, the fact remains that most victims of cyber fraud do not benefit from it. Lack of awareness of cyber cells is the reason for their passive state.

- E-consumer are dependent on the passive response of these cyber cells for remedy and it is a noticeable thing that the procedure and solution of the cyber cell take time to bring in the remedy to the cyber victims, particularly in e-banking and online financial fraud, in a really strict implementation. E-consumer does not want to be involved in the legal procedure because of the very slow procedure and lack of active authority to hear cyber victims. In the COVID-19 pandemic situation maximum, consumers are doing the digital transaction, the e-commerce market has reached on new growth. In this pandemic, a lot of cyber frauds case under PM Cares Fund, debit/credit card and hacking cases are registered but people could not get justice against cyber crimes.
- Development of e-commerce gave a chance to cyber criminals to use the internet for illegal activities, so there is a need for a strong legal structure to control illegal activity on the internet. Hence it is strongly suggested to make law in the form of a treaty or convention under the agency of United Nations, which wholly covers all elements of known and possibly illegal activities committed on, or with the assistance of the internet. Moreover, this treaty should include important clauses discussing various jurisdictional issues applicable to all the signatory countries. Any nation's access to the Internet should be made contingent

upon that country's signing and ratification of such a treaty or convention.

- It is proposed to insert a new section or new act applied to the Constitute of Digital Consumer Courts (DCC). The principle of natural justice requires a fair and speedy procedure for the dispute of online consumers. Constitute of Digital Consumer Courts (DCC) can play a very positive role to implement principles of natural justice to consumer disputes in cyberspace. In order to this, there is a need for a digital healing mechanism; there must be an establishment online Consumer Court particularly to deal with frauds and crimes with consumers in e-Commerce.
- There should be a cyber security expert team in Digital Consumer Courts (DCC) with experts in cyber law can be constituted in existing consumer courts. The qualification of appointing authority of the cyber expert team should be clear and must be complete information regarding the qualification, appointment, criteria of age, salary, terms of service, termination, powers and functions of members of Digital Consumer Courts (DCC). This is a composite strategy to deal with digital commercial disputes both in the offline world and the virtual world.
- The consumer is a king is not totally correct, he is a more vulnerable party in electronic commerce as the terms of contracts are dictated by one party (seller) and these are accepted by the other (consumer). It is suggested that (a) it must be made mandatory for all online commercial websites to display contract information logically on their home page of the website, (b) the e-commerce platforms must have authentication from Trust Pay and such other authenticated systems and (c) businesses must take a vital role in delivering all the terms and conditions of the online contract whether by messages, fax, e-mail and phone communication.
- To control computer crimes, one is required to understand them in the perspective of technological advancements and the ease with which they

can be committed. The old maxim of the deterrent theory of punishment 'an eye for an eye' should be equally applicable to reduce computer crimes. It should be 'technology for technology'. If anyone is committing a crime by using the internet, one will be blocked to do so by using technology itself. Law can merely reduce but cannot supplement the effort of deterring a cyber-criminal.

- Every country, including India, must endeavour to draft a complete Cyberspace Law, which inter alia also addresses issues relating to infringement of e-consumer rights on the internet. E-commerce disputes issue in cyberspace is a technical and legal issue that cannot be dealt with by simply extending the scope of traditional laws. All the available case law shows that e-commerce law needs a foundation to resolve disputes in cyberspace. Courts, particularly in India however, need to consider policy implications because the Internet is a new medium of communication that forces e-commerce law to evolve. Moreover, the significant differences between e-commerce law requirements and traditional commerce law that traditional laws are not a capable to give remedy for e-commerce issues. There is a need for technical aspects in law that must be given due weight and appropriate treatment while framing the relevant provisions in the Cyberspace Code.
- Consumer protection issues in the era of e-commerce have gained a considerable amount of attention both from academicians and policy-makers. Furthermore, governments, as well as an intergovernmental organization, have discussed the issues involved and developed various frameworks. But a review of the existing legal framework shows that it has failed to address the e–consumer needs. The Consumer Protection Act, 2019 specifically excludes from its ambit the rendering of any service that is free of charge. Assume that the online platform is not taking any charge to the users; the newly enacted Consumer Protection Act, 2019 does not apply to free products and services. E-commerce sites always give free service as an offer with the product. We can

always see the offer that "Spean the wheel and try your luck, you will get free item" "give the answer of below question and get attractive items free of the cast" The law and e-commerce policy are still considerably far from the goal, so consider protecting e-consumer rights in the law and providing remedies and security for all online services and products for electronic consumers.

- The appointment of members in the new Consumer Protection Act, 2019 wholly depends on the power of central government. There is no provision for the Selection Committee. The central government will appoint through notification. It means that non-judicial member or anyone may be appointed as a member of the redressal body. While in the 1986 Act there is a provision of Selection Committee (composition a judicial member and other officials) who recommend members on the Commissions. It resulted in a conflict of interest that could arise when government nominees hear cases involving a government entity. So the government should take notice of this provision.
- Healthcare is now one of the most important sectors in India, both in terms of income and employment. Healthcare includes hospitals, medical devices, clinical trials, outsourcing, tele-pharmaceuticals, medical tourism, health insurance, and medical equipment. India's health sector is growing at a rapid pace thanks to the increased coverage in services and increased spending of the public and private sectors. A large number of consumers are working or taking services in this sector but in India, there is no legal provision available to protect e-consumer rights in this area. Even in the newly enacted consumer protection act, healthcare services are not addressed in the list of services. So it is highly recommended that the health care sector must be defined and consumers' rights of this sector should be properly addressed in policy and law.
- In the present situation, the e-commerce sector has a most troubling situation with the growing practice of automatic contract changes

without consumers understanding and consent. This system should be strictly banned as the service and goods provider can sometimes alter the terms and conditions at any time, without notice to consumers, simply by posting a particular sentence of the modification. Furthermore, the term and condition on the e-commerce website are written in very small font and not in the form of regional language. This situation is highly disparaging of consumer rights and drains their confidence in electronic commerce.

- In this study, it is humbly submitted that the Indian Contract Act 1872 is a boost to the Information Technology Act 2000 (2008) and if a question or doubt arises on the validity of the contract online, then a fair decision is made by giving harmonious construction to the two laws. But it is argued that India's Contract Act 1872 was made about 148 years ago, except for minor changes which have been made along the years. It was structured according to society and market and keeping in mind the nature of business transactions. The illustrations cited in the law are inconsistent with the situations of digital contracts. Hence, the legal provisions for a valid online business contract should be updated and the latest illustrations should be added in the Information Technology Law, 2000 (2008), in order to make the IT Law a complete guide in itself for every situation arising from e-commerce.
- Compliance for e-commerce is dependent on key factors namely, ICT infrastructure, legal and financial framework. The research has shown that clear-cut implementation strategy and its effective administration are important and mere announcement of intention is insufficient for the promotion of e-commerce and consumer protection. Digital India program, encourages e-payment system, BHIM or other e-wallets, which are no doubt all methods which facilitate consumers to save time, save money, anywhere and anytime. However, without the proper infrastructure and without proper redressal system in e-payment and

proper technically literate consumer, how can one assume a secured e-payment system.

- Nowadays a lot of cases are happening in e-payment methods like card cloning, auto deduction of money from e-wallets, OTP cheating, issues in the use of debit/credit card in swipe machine. There is also a severe issue of delay in processing of banking system although reserve bank has set the limitation. Moreover, in several cases banks are not interested to take issue in e-payment if the consumer is an ordinary person with no contacts or connections and the amount deducted is some hundred or some thousand rupees only. The banking process is also exhausting with unlimited enquiries by the bank that move slowly, step by step. So consider the above mentioned situation, the government should make a sufficient law to handle e-payments mechanism and set protection measurements, the process of complaint in the banking system must be seen on a real ground level, not in books. The mere announcement of the intention of law or encouraging the consumers by words is not sufficient, implementation of the law on the ground should be seen.
- Data Privacy protection is a critical element of e-consumer and user trust in the digital environment and a necessary condition for the growth of electronic commerce. Unfortunately in India despite of much technological development, there is no law or policy for the protection of data privacy. In India, many consumers have never had access to the Internet via a computer or tablet. Such consumer is connected with the Internet occurs only via smart phone. When Indian consumers use Internet services, social media, and other such applications, they transfer their personal data to service providers in exchange for the free use of their services. And these data are usually stored on servers outside India’s borders, which is a very sensitive and dangerous issue for the consumer and the Indian government. In this regard the following suggestions may be beneficial if authorities adopt:

If the company wants to store data collection of consumers, it needs to fulfil the following:

- The data subject must be informed.
- Notification about what information has to be collected and for what purpose and the possibility to choose whether or not to accept the collection and use of the data.
- The data must be collected for specific, explicit and lawful purposes.
- The data collected must be adequate, reliable and not excessive in relation to the purposes for which it is obtained.
- The data must be used only for the purposes for which they were collected and must not be used or disclosed in a way incompatible with these purposes.
- The data must be stored in a form that allows identification of the interested party in addition to what is necessary for the purposes for which the data were collected.
- The party that collects and stores the data is required to ensure its accuracy and keep up to date; all reasonable steps must be taken to ensure that inaccurate or incomplete data is corrected or deleted.
- The server who is located in a foreign country is obligated to give the server provider access to that country where he has business and collect a lot of revenue like Facebook, Whatsapp, Twitter etc. Recently, an exponential violation of data privacy was noted in the case of Facebook Cambridge Analytica.
- The whole world of e-commerce is techno-legal as well as social so e-commerce involves all groups of society, law and technology. Due to this aspect, the judiciary in India is not capable of deciding e-commerce cases so it is suggested that a technical training course for judges should be provided and there should be a techno expert panel to assist the judges which provide a speedy trial in cyber cases. It

may be noted that there is no case law available of the Supreme Court in India in this regard.

- United Nations should come forward for the establishment of the International Court of E-commerce (ICE) because it involves all countries in e-commerce transactions. Jurisdiction issue in e-commerce is much complicated and we always find that state enter into conflicts because each country has their own legal infrastructure and set of rules. The e-commerce transaction is a subject of trans-national law with zero limitation and no country allows the enforcement of the judgment of the foreign court in the absence of ant treaty or Convention. So the UN needs to make uniform laws like UDHR and establish an International Court of E-commerce (ICE) to resolve jurisdiction issues and states conflicts.
- Religious, social and obscene misleading advertisements are spreading much on television, internet, smart phone, and social media. One example can be that most broadcasters are broadcasting Babas, astrologers, hakims and ayurvedic doctors who claim for their magical and miracle treatment of grahdosh and serious deceases like cancer, tuberculosis. Despite many laws to stop misleading advertisements, nothing has happened in this regard. The new Consumer Protection Act, 2019 defines misleading advertisements but misleading programs are not including in misleading advertisements. In the lack of proper implementation of the law, the immoral, misleading advertisements and programs are continuing to go on without any fear. So one may need a strong mechanism to regulate television, internet, smart phone and social media in this regards. The mechanism should also be responsible for any content of misleading advertisements and programs.
- The second-hand C2B consumer is not measured as a consumer; the law does not protect a consumer who has sold or buys the used product under the newly enacted consumer protection law, whereas

all c2b e-commerce companies like OLX, Cashify, Cars 24 are getting much revenue from consumers. This model is rapidly growing in the new age of e-commerce. So it is humbly submitted that there is a requirement to enact a law or put in place a policy that protects the rights of such consumers.

7.3.2 Suggestions Regarding E-Consumers

E-commerce brought a dynamic change in the consumer's life; it has changed the way of shopping and thinking. With every need people first think about the internet, if we think about shopping immediately we open Flipkart, Amazon and other shopping sites, if we feel bored we immediately open social media or YouTube and share information and pictures without thinking about the associated risk or danger. Thus, it has resulted in the loss of our personal information, money, blackmailing and many other risks. The following suggestions would be beneficial for consumers and society:

- Do not make any transaction over public shared computers or while using public Wi-Fi networks. These computers may have key loggers installed that are designed to capture keyboard input and could allow scammers to steal your username and password.
- Never disclose your net bank password, your unique password (OTP), your bank or bank phone PIN, your CVV number, your expiration date to anyone, even if it claims to come from your bank. Also, never respond to emails asking for the above details that appear to have been received from your bank.
- Bank or its employees will never call, message or email requesting your net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number, etc. if such cases happen, it should be immediately reported to the bank.
- Always use strong passwords, and prefer separate ID/password combinations for different accounts so no one can find you. Change your online bank passwords regularly.

- To make passwords strong, use in upper case and lower case alphabets, numbers and special characters. Never use simple passwords like Jan@2018, yourname@000, password@computer, use date of birth, etc.
- Always use virtual keyboards at the time of using internet banking services. Particularly performed in case we need to access a net banking facility from a public computer / cyber café or from a shared computer.
- Never make any financial transactions on shared public computers or while using public Wi-Fi networks. These computers may have key loggers designed to collect keyboard input and allow fraudsters to steal your username and password.
- Remember to log out of your online banking portal/website after completing your credit/debit card transaction online. Always erase your browsing information like history, password, and cookies (Internet Explorer, Chrome, Firefox, etc.) after completing your online banking activity.
- Always be sure about the correct address of the bank website and look for the 'lock' icon on the browser's status bar and check the colour of lock icon, green colour means it is a safe website, while you visiting your bank's website or conducting an online transaction.
- Always make sure that 'https' appears on the address bar before doing business online. 'S' stands for 'secure' and indicates that communications with the website are encrypted.
- Keep your bank's service number handy so that you can immediately report any suspicious or unauthorized transactions to your account.
- Criminals can easily send compelling emails that appear to come from your bank. Do not click on the links provided in this email

even if they are genuine. You may be directed to a malicious website..

- When you receive your credit/debit card from your bank, make sure the letter is not damaged and properly sealed. If there are any signs of tampering with the package, please notify your bank immediately.
- Make sure to change your credit/debit card PIN when you receive a new card from your bank. You can change your PIN online on your bank's website or at your local ATM.
- Make sure to swipe your credit or debit card in front of you to avoid duplicate / illegal copying of your card information. Don't force shopkeeper to swipe cards to cancel a transaction.
- Be especially careful when entering your password / PIN code so that no one can see it. Cover the keyboard with your other hand while entering the PIN to prevent anyone from watching through the CCTV from taking your number.
- Register your personal phone number with your bank and subscribe to cell phone notifications. These notifications will notify you immediately of any suspicious transactions and failed attempts to connect to your net bank account.
- Always check the transaction notice received on your registered mobile phone number and make sure the transaction is billed based on your purchase.
- Keep an eye on the people around you when you make an ATM transaction. Make sure no one is too close to you when you make a transactions with an ATM. You must keep your PIN secret and close the transaction completely before leaving the ATM. If there is something suspicious, cancel your transaction and leave immediately.
- Activate the international transaction option on your credit card only if you travel abroad. Always make sure that the international

transaction option on your card is disabled when you return to your country.

- Fraudsters can call members of your family who claim to be hospital staff and request a money transfer that claims to have had an accident and desperately need money. This could be spam. Before accepting this request, contact your family member to confirm where he is and verify the authenticity of the call.
- Keep your Smartphones up to date with the latest software operating system if you are using your mobile phone for online banking. Regularly check your smartphone for the update. To update your smartphone, go to about the phone option in setting menu and click on the software update option. Always install a good antivirus as well and keep it up-to-date by enabling the automatic update feature in your smartphone.
- Always ignore suspicious advertisements if it claims that you can earn money with little or no work or you can make money on an investment with little or no risk or share this link to others and get a free lot of reward.. It could be a scam. These offers seem, too good to be true, but you may end up losing hard-earned money.
- Always use well-known websites for online shopping rather than shopping by searching for products on search engines. Any search results can be misleading and may lead to malicious websites. Avoid using third-party extensions, plugins or add-ons for your web browser as it may secretly track your activity and steal your personal details.
- Always check and install authentic wallet apps directly from the App Store on your smartphone. Do not follow links shared via email, text or social media to install wallet apps.
- Do not share your card or bank account details in your electronic wallet, as this increases the risk of theft or fraudulent transactions in the event of a security breach.

- Always enter information in online forms and do not use the auto fill option in your web browser to fill in online forms, as they may store personal information such as card number, CVV number, bank account number, etc.
- Try to remember your card CVV number or write it on safe place and strikeout and color the CVV number with a permanent marker. There will be no problem with the card if you do such, CVV number required only at the time of online shopping, never required for offline purchasing. If any offline sales person asks you for your card CVV number, never disclose it.
- Never handover your smart phone to any stranger or to an unknow person. Your smart phone can be hacked within only 20 second. Hackers install APK file which you can never see in your device. You can never imagine that your smart phone is actually active and properly operated while your phone status is switch off. Hackers can use camera, microphone and may continue watching you, no matter where you are.
- It is suggested to consumers that the use of keypad phone is safest way of online transactions because keypad phone does not support any 3G, 4G network and you cannot access internet facility. Hacking or online thieves are not possible on keypad phone. So the mobile number which is registered with UPI or bank, should be used on a phone with a keypad.

7.3.3 Suggestions about Using Social Media Platform

Social media attention is increasing worldwide. A phenomenal increase in the use of social media platforms, social network environments provided a prolific ground for cyber criminals to engage in illegal activities. Some well-known social media platforms are Facebook, Twitter, Instagram, YouTube, LinkedIn, WhatsApp, Snapchat, Hike, WeChat, Tumblr, OkCupid, TikTok, Tinder, etc. following some important tips everyone should take to protect himself and protect information at the time of using social media platforms:

- Never accept friend requests from unknown people and also do not send friend requests to any unknown people on social networking sites.
- Don't respond to any messages on social networking sites, if the sender is unknown and the message includes any link, attractive thing or emotional moral talking. Block immediately such sender and repot social networking sites if you think the message has anti-social, hate speech, obscene content.
- Maximum online users are fake and have fake information in their profile so don't trust such people. Respond to online users only when you know them and can trust them in real life.
- To share your personal information such as an address, phone number, date of birth, your family photos, about your future plan and about your travel on social media, may be a big privacy risk and sometimes as a crime. Hackers, companies, cyber criminal can use your shared information against you. So don't share any personal information on social media, think hundred times before sharing.
- If you notice that a fake account has been created by using your personal information and your profile picture seems to have changed or if you have received and sent unwanted bulgur messages, it means that your profile has been hacked. In this situation immediately inform the social media service provider and tweet your problem on *@Cyber Dost.*
- Location services on your devices should be turned off; use your location service only when it is necessary. Hackers can easily access your situation if you keep your location always on.
- Always select the right privacy settings on social media websites. For this go to the setting menu and choose the privacy setting option. After selecting the right privacy setting you can share videos and photos.
- Your password should be of minimum ten words and make your password by using alphabets in upper case and lower case, numbers and

special characters for your social media account. Change your password in a month once and also if you think your password may have been disclosed or others know about it.

- You should not allow social networking sites to access your email account to look for your friends and send spam emails to them without your consent or knowledge.
- If you are talking online with someone and if you are doubtful on your conversation partner, attempt to ask related scientific or mathematical questions. If you do not get the answer or acknowledge the question, it may mean that you are chatting with an automated computer robot. This system called an AI system like *Alexa* and *Google assistant*. So try this method to identify doubtful online chats.
- To access social networking websites, you need not go to a public computer, cyber cafe or public *wi-fi*. It may be infected/ installed with a key logger application that will capture your keystrokes including the login details.
- Many social networking sites may direct you to download a third-party applications that may let you access more pages. Do not download unified third-party applications without knowing about its safety. You may have noticed on social media platforms that third-party applications like face changer, know your last life, how you see in old age, etc always show on your profile.
- Always report offensive posts, anti-social and abusive content on social media. The authority never discloses your details if you file a report.
- Do not share or forward unverified, fake posts, news, videos and messages on social media platforms. Such a post contains fake news or contains sensitive information that may mislead people. Maximum riots or mob lynching crime happen due to the circulation of such a post. To share such posts may lead you in committing a crime and you may become liable for punishment. So if you get such a post, immediately report to authorities for action.

Today, Whatsapp is the most popular messenger service. In WhatsApp, chats save in the app during the day and in its cloud storage at night time. WhatsApp chat is encrypted but content saved on the cloud is not encrypted. Thanks to end-to-end encryption technology, WhatsApp is considered the most secure messaging platform. Despite this, many times the news of chat leaks or viral gets heard. Recently, in the Sushant murder case, WhatsApp chats of some stardom spread viral, after which many issues were asked about the safety of the social media platform in the minds of people. No hacker will be able to leak WhatsApp chats, just one has to to take care of these five things as stated below. Only few know that WhatsApp offers its users a variety of security features. To keep your account secure, WhatsApp users must need to understand certain rules so that the personal talks does not fall into the hands of cyber criminals. The following steps keep you safe and secure :

i. Disable Cloud Backup

At night, WhatsApp stores all daytime conversations in cloud storage. This is because, if the user uninstalls WhatsApp or opens an account on a new phone, then cloud chat can recover old chats and media files. The thing to keep in mind is that the WhatsApp chat is encrypted, but the content saved in the cloud is not encrypted. In such a situation, if access to a backup falls in the hands of a hacker, he can easily back up the WhatsApp chat to another device and it can easily be read. If you are afraid that WhatsApp chat will fall into the wrong hands, immediately turn off the automatic cloud option.

However, if you uninstall WhatsApp, you will not be able to restore the old chat by reinstalling the application. Use these steps to disable WhatsApp Settings> Chats> Chat Backup>Back up to Google Drive option> select Never

ii. Manual Encryption Check

Although WhatsApp chat is encrypted, we can check it ourselves. To check, open the chat and click on the name and then click on the encryption option. After tapping, a pop-up will appear, showing the QR code and 40 digits below. This is the security code. This is WhatsApp Identity, which can be shared with others as well. If you want to make sure that your WhatsApp chat is secure or not, then you can verify the code shown on your phone with another user's code. Follow these steps to select WhatsApp settings > Chat s> Backup chat>Backup to Google Drive>select Never for encryption.

iii. Two-step verification

2-step verification can improve account security. If you enable this feature, you will be asked for a six-digit code that only you know. Each time you open an account on another device, you need to enter a six-digit code. In one situation, even if a hacker finds your WhatsApp number or account details, they can't use WhatsApp because they need a six-digit code to use it. To activate it, follow these steps Menu> Settings>Account> Two-step verification> Enable.

iv. Active Fingerprint / Face-ID Security

WhatsApp Users can protect WhatsApp with their fingerprints or Face-ID. Android users follow these steps to enable Settings> Accounts> Privacy> Fingerprint Unlock. Likewise, Apple users can activate Face ID.

v. Don't Get Caught in a Scam

Last but most important rule, don't click on any unknown link that enters the WhatsApp group without thinking. It may be spyware that can hijack personal information from your device. Also, do not download files sent to your inbox from an unknown number. However, to avoid this, the feature is available on WhatsApp. Because of this role, you can decide without your permission who can add you to group and who cannot. To do this follow these steps Settings> Account> Privacy> Groups> My contact.

BIBLIOGRAPHY

BIBLIOGRAPHY

BOOKS

1. A Gatt, "*The Enforceability of Click-wrap agreements*" (Computer Law & Security Report,2002 408).
2. Aashit Shah and Parveen et. al., *Legal issues in E-commerce* **,** (Nishith Desai Associates),
3. Al-Rasheed, and S., Zairi, *et. al, A.M. Getting in the Mind of the Customer: An Empirical Study of Consumer Behaviour in Retailing.* (Bradford University, 2004).
4. Alwyn Didar singh, *E-Commerce in India: Assessments and Strategies for the Developing World,(* lexix Nexix Butterworths,2008).
5. J. Christopher Westland & Theodore H.K Clark., Global *Electronic Commerce-Theory and Case Studies 1(*MIT Press, 2nd edn., 2000).
6. Cram M. Carol, *E-Commerce Concepts 2,* (Illustrated Series, Course Technology, 2001)
7. Dave Chaffey, *E-Business and E-Commerce Management: Strategy, Implementation and Practice*, (Pearson Education 3rd edn., 2013).
8. David Whiteley , *E-Commerce: Strategy, Technologies and Applications*, (Tata McGra-Hill Company Limited, 1st Edition 2001).
9. Deitel Harvey M, E-*Business & E-Commerce for Managers*,(Pearson ISBN: 9788131760680, 9788131760680)
10. Dennis Abrazhevich, *Electronic Payment Systems: a User-Centered Perspective and Interaction Design,* (J.F. Schouten School for User-System Interaction Research, Netherlands, 2004) (Ph.D. Thesis).
11. Efraim Turban, Jae Lee, David King, H.Michael Chung, "*Electronic Commerce–A Managerial Perspective*", (Pearson; 4th edn. ,December 12, 2016)

12. Elias M Award, *Electronic Commerce from Vision to Fulfillment*, (3rd edn., Prentice-Hall of India Pvt.Ltd)

13. Elias. M. Awad, " *Electronic Commerce From Vision to Fulfillment 12-1* ", (Prentice-Hall of India Pvt Ltd, 2007).

14. Gary P. Schneider, *Electronic Commerce*,(Cengage Learning Customer & Sales Support, 9th edn. 2011)

15. Hemant Goel, *Law & Emerging Technology* (Jain Book Depot, (2010).

16. J. Miller and Brian W. Harvey, et. al. , *Consumer and Trading Law: Text, Cases,and Materials*, (Oxford University Press,1998)

17. Janice Reynolds, *The Complete E-Commerce Book: Design, Build, & Maintain a Successful Web-based Business*, (2nd edn. CMP Books © 2004).

18. Jill Dyche, *The CRM Handbook Addison* (Wesley Professional; 1st edn. (August 9, 2001).

19. Joga Rao, *Computer Contracts and Information Technology Law*, (2nd edn.., vol. 1, Wadhwa & Co.,Nagpur, 2005)

20. Judy Strauss, Adel El-Ansary, Raymond Frost, "*E-Marketing*", 3rd edn., (Prentice Hall- Gale,2002)

21. Juon Catherine, Internet Marketing Start to Finish, (Pearson, ISBN: 9788131786949, 9788131786949)

22. Kenneth C Laudon and Carol Guercio Traver , *E-Commerce: Business, Technology, Society*, (Pearson, 4th edn. 2008).

23. Kamlesh K Bajaj. & Debjani Nag, *E-Commerce- The Cutting Edge of Business* (Tata McGraw-Hill Publishing Company Limited, 2nd edn. 1999).

24. Kevin M.Rogers, *The Internet and the Law* (Palgrave Macmillan, 2011).

25. Lilian Edwards and Charlotte Waelde (eds.), *Law and the Internet: A Framework for Electronic Commerce* (Hart 2000).

26. L Padmavathi, E-*Commerce: Consumer Protection* (ICFAI university press,2008)

27. Michael Chissick and Alistair Kelman, *Electronic Commerce: Law and Practice* (London: Sweet & Maxwell, 1999).

28. Nandan Kamath, *Computers Internet & E-Commerce*, (4th edn., Universal Law Publishing Co. ,2009).

29. P. Timmers, *Electronic Commerce – Strategies and Models for Business-to-Business Trading* (John Wiley & Sons, 2000).

30. Peter B. Maggs, *Internet and Computer Law: Cases – Comments – Questions* (St. Paul, MN: West Group, 2001).

31. Paul Siegel, *Communication Law in America* (Rowman & Littlefield, 2011).

32. Ratanlal & Dhirajlal, *The Law of Evidence*, (21st Ed., Wadhwa & Co., Nagpur, 2009).

33. Ravi Kalakota and Andrew B. Whinston, "*Electronic Commerce-A Manager's guide*", (Addison-Wesley Professional; 1st edn. January 2, 1997).

34. Richard T. Watson and Pierre Berthon *et.al*, *Electronic Commerce: The Strategic Perspective*, *(*The Global Text Project is funded by the Jacobs Foundation, Zurich, Switzerland,2008)

35. Robert Dunne, Computer and the Law: An Introduction to Basic Principles and Their Application in Cyberspace, (Cambridge University Press, 1st edn., (2009)).

36. Rodney D. Ryder's, Introduction to the Internet Law & Policy, Wadhwa and Company, 1st ed., (2007).

37. Rwal, Nidhi, *Consumer Redressal Seeking Behaviour with Reference to Services Extended by Indian Railways*, (Vadodara: The Maharaja Sayajirao University of Baroda, 2003. (Ph.D. Thesis).

38. S. K. Verma and Mittal Raman, Legal Dimensions of Cyber Space,(Indian Law Institute ,(2004).

39. Seth Karnika, *Cyber Laws in The Information Technology Age* (Lexis Nexis Butterworth Wadhwa, 2009).Sharon K. Black, Telecommunications Law in the Internet Age, (San Francisco: Morgan Kaufmann, 2002).

40. Takashi Kubota, Cyber *law for Global E-Business: Finance, Payments and Dispute Resolution*, (Information Science Reference, New York ,2008).

41. Shubhashish Gangoupdhyaya , *Waiting To Connect* (Butterworths India, 2013) .

42. S. Dayal, *The Internet*, (Butterworths,1997).

43. Tran Van Hoa(ed.), *Advances in household economics, consumer behaviour and economic policy*, London: (Ashgate, 2005).

44. Janice Reynolds, *The Complete E-Commerce Book: Design, Build, & Maintain a Successful Web-based Business*,233 (CMP Books, 2nd edn., 2004)

Articles

1. Akomolede T.I “Contemporary Issues in Electronic Commerce in Nigeria’’ 113 PER/PELJ (2008)

2. Angshuman Hazarika, E.Commerce*: “*Expectations and shortfall*”* 2 Christ University Law Journal 59- 78((2013)) ISSN 2278 – 4322/doi.org/ 10.12728/culj.3.

3. Arthur, Brian. "Increasing Returns and the New World of Business." *Harvard* Business *Review* (July-August 1996).

4. Ashok Panigrahi and Ranjan Upadhyaya, *et.al*.(eds.). “E-Commerce Services in India: Prospects and Problems’’, IJTEP, 15-22 ,(2016)

5. Ayo C.K, and Adewoye J, *et.al* (eds.), "Business-to-consumer e-commerce in Nigeria' Prospects and Challenges'', 5109 AJBM.
6. B Mahadevan, "Business Models for Internet based E-Commerce: An Anatomy", California Law review, (vol.42, 2000)
7. Bansal, Rashmi,"Growth of the Electronic Commerce in China and India: A Comparative Study" Journal of Asia-Pacific Business, 356-374, (vol.12,2011
8. Baranoff, R.M., P.F. michalak *et al.*, "Set your sites high", LIMRA's Market Facts, 30-44 (vol. 16, 1997)
9. C. M. ABHILASH, "E-Commerce Law in Developing Countries: An Indian Perspective, Information & Communication Technology Law,11:3, 269-281, DOI: 10.1080/1360083022000031948
10. Compbell, A.J., *Ten Reasons Why Your Business Should Use Electronic Commerce* pp. 12-14.(Business America, 1998).
11. Chanana Nisha and Goele Sangeeta, "Future of E-Commerce in India", International Journal of Computing & Business Research ISSN (Online), 2229-6166 (2012)
12. Cindy Chen, "*United States and European Union Approaches to Internet Jurisdiction and Their Impact on E-Commerce"*, 25 U. PA. J. INT'L L. 423 (2004).
13. Carmen Nadia "Integrating Digital Economy and Green Economy: Opportunities for Sustainable Development" TERUM (volume 6, issue 1, February ,2011).
14. Deepa Verma1 and Harita Mehla, "A Study on E-Commerce – Conceptual Framework & Future Potential in India", IJ EMSP, (Vol. 13, Issue 01, March 2014).
15. Dr. Shahid and Kansana, Keshav "A Review Paper on E-Commerce" *available at* https://www.researchgate.net/publication/304703920 (vol. 2, 2016)

16. Dr. Shahid and Kansana, Keshav and Majid, et.al.(eds.) "A Review Paper on E-Commerce", inproceedings, (2016)

17. Dr. shashi nath mandal, "E-Marketing" GJMBR, (vol.16, 2010)

18. Dubey Rahul, "E-Commerce poised for a leap in 2012" *available* at https://www.exchange4media.com/digital-news/e-commerce-poised-for-a-leap-in-2012-44890.html

19. Emmanuel Lallana and Rudy Quimbo *et.al*(eds.), "e Primer: An Introduction to e-commerce'' ,IJCSMC 109 – 111, (Vol. 5, 2016)

20. Gary Gregory, Munib Karavdic and Shaoming Zou, "The Effects of E-Commerce Drivers on Export Marketing Strategy, Journal of International Marketing" 30-57, (Vol. 15, No. 2 (2007).

21. Gary P. Schneider, *Electronic Commerce*,18 (Cengage Learning Customer & Sales Support, 9th edn. 2011).

22. Herekar M. Prakash " Ecommerce in India – Problems AND Prospectus, ASM International" E Journal Ongoing research in Management and IT.

23. Hutchinson, "Can trade mark protection respond to the international threat of cybersquatting?'' Journal of Information, Law and Technology (vol 1, 2001).

24. Justice S. Muralidhar, "Jurisdictional Issues in Cyberspace" IJLT, (vol. 6,2010).

25. Jill Ellsworth H. & Matthew V.Ellsworth, *The New Internet Business Book*, 3 (John Wiley & Sons, Inc., 1996)

26. Kaur Pradeep, Dr. Joshi Mukesh, E-Commerce in India: A Review, IJCST (vol. l. 3, issue 1, 2012)

27. Kaur, Ramneet, E-Commerce in India, Asian journal of research in business economics and management, (vol. 2, issue 6, 2012)

28. *Koolwal, Mahesh* , "*Consumer Jurisprudence*" NALSAR *Law* Review. (vol. 13; 2004)

29. Kshetri Nir "Barriers to ecommerce and competitive business models in developing countries: A case study. Electronic Commerce Research and Applications", 443–452, Vol. 6, Issue 4, (2015)

30. L.C. Leung, W. Cheung, Y.V. Hui, "A framework for a logistics ecommerce community network: the Hong Kong air cargo industry" IEEE *T Systems, Man, and Cybernetics Part A: Systems and Humans.*, (2000) .

31. Nuruddeen, Muhammad and Yusof, Yuhanif and Abdullah, *et.al* (eds.), "Legal Framework for E-commerce Transactions and Consumer Protection: A Comparative Study" BJPCL, 41-56, BJ, (2016)

32. Ogundele, Gboyega, "Developing Legal Framework for Electronic Commerce in Nigeria: Some Lessons from U.K and Singapore" (May 21, 2018).

33. Peter Cunningham and F Friedrich roschl, *Electronic Business Revolution* Springer 15 (Verlag, 1999).

34. R. C. Arnett, "Communication and community: Implications of Martin Buber's dialogue". Carbondale, IL: Southern Illinois University Press, (1986).

35. Raj, Aijaj and Rahman, Wazida, "E-commerce Laws and Regulations in India: Issues and Challenges" 44-51, researchgate.net (vol.1 2016).

36. Rajesh Chakrabarti & Vikas Kardile, *The Asian Manager's Handbook of E-Commerce*, 9 (Tata McGraw Hill, New Delhi, 2002)

37. Raj, and Aijaj, et.al.(eds.),"E-commerce Laws and Regulations in India: Issues and Challenges'',(vol.1,2016) https://www.researchgate.net/publication/330845555

38. Rania Nemat, "Taking a look at different types of e-commerce", WAP, 101-104, (vol (1), 2012)

39. Rosen, Anita, "The E-commerce Question and Answer Book'' USA: American Management Association,5, (2000).

40. Sandeep ladda, "E-commerce in India Accelerating growth" PD 325, (February 2015)

41. Sarbapriya Ray, "Emerging Trend of E-Commerce in India: Some Crucial Issues, Prospects and Challenges", CEIS, (vol. 2, No.5, 2011)

42. Sharma Rama and Ms. Srivastava Vibha, *et.al*. (eds.), "Consumer Protection in the Era of E-commerce", IJR (Vol-1, Issue-8)

43. Yaser Ahangari Nanehkaran, An Introduction To Electronic Commerce, IJSTR (vol. 2, April 2013).

44. Yazdanifard, and Prof. Dr. Rashad *et.al* (eds.), "The Evolution of Internet Marketing: Holistic Diagram of Underlying Theories" AIEIWRWTES, 761-769 (vol.80, 2012)

BARE ACTS

INDIAN ACTS

- The Information Technology Act, 2000
- The Information Technology (Amendment) Act, 2008
- The Consumer Protection Act, 1986
- The Consumer Protection (Amendment) Act, 2002
- The Consumer Protection Act, 2019
- The Consumer Protection Rules, 2019
- The Indian Contracts Act, 1872
- The Indian Panel Code, 1860
- The Personal Data Protection Bill, 2019

INTERNATIONAL ACTS

- UNCITRAL Model Law on Electronic Commerce,1996
- The United Federal Trade Commission Can-Spam Act, 2003
- Anticybersquatting Consumer Protection Act,1999
- The Hague Conference on Private International Law
- Singapore the Electronic Transactions Act of 1998
- United Nations Guidelines for Consumer (UNGCP)

DOCUMENTS

- The Hague Conference, 1995
- Brussels Convention 1968
- Brussels I Regulation
- WTO Convention on the Law Applicable to Contractual Obligations
- European Union Directive, 2000
- Hague Convention on choice of court Agreement 2005
- The American Bar Association (ABA**)** subject matter jurisdiction
- United Nations Convention on Contracts for the International Sale
- UNCITRAL Model Law on Electronic Signatures
- UN's Sustainable Development Goals (SDGs)
- United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)
- The Asia-Pacific Economic Cooperation (APEC) policy on e-commerce
- International Chamber of Commerce (ICC)
- OECD Consumer Protection Guidelines, December 1999
- Razorpay report on The Impact of COVID-19 on E-commerce in India
- https://www.researchandmarkets.com report on the Impact of COVID 19 on the e-commerce Market
- Guidelines for Intermediaries and Digital Media Ethics Code Rules of 2021

- WhatsApp new privacy Rule, 2021

NEWSPAPERS

- The Times of India
- The Economic Times
- The Indian Express
- Dainik Jagran
- Hindustan
- Amar Ujala
- Dainik Bhaskar

LIST OF WEBSITES

1. www.pwc.in
2. https://www.bigcommerce.com/blog/types-of-ecommerce-business-models/
3. https://www.ecommerceceo.com/types-of-ecommerce-business-models/
4. https://www.tutorialspoint.com/e_commerce/e_commerce_business_models.htm
5. https://www.eyerys.com/articles/types-e-commerce-models
6. https://www.numinix.com/blog/2018/11/05/what-are-the-different-categories-of-e-commerce/comment-page-1/
7. https://wikidiff.com/transition/transaction
8. https://www.welchllp.com/blog/what-is-a-business-transition/
9. https://en.wikipedia.org/wiki/Database_transaction
10. https://cybercrime.gov.in/pdf/Safe%20Use%20of%20social%20Media%20Platform%20Brochure%20final.pdf
11. https://cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20final.pdf

12. https://www.oapen.org/download/?type=document&docid=391038
13. https://globaljournals.org/GJMBR_Volume16/3-Electronic-Commerce-A-Study.pdf
14. https://www.oapen.org/download/?type=document&docid=391038
15. https://cis-india.org/internet-governance/publications/jurisdictional-issues/at_download/file
16. https://shodhganga.inflibnet.ac.in/bitstream/10603/188821/10/8%20chapter%206.pdf
17. https://www.law.upenn.edu/journals/jil/articles/volume25/issue1/Chen25U.Pa.J.Int'lEcon.L.423(2004).pdf
18. https://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=5651
19. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/1079.pdf
20. https://repository.jmls.edu/cgi/viewcontent.cgi?article=1120&context=jitpl
21. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009945
22. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42090
23. https://journalofbusiness.org/index.php/GJMBR/article/download/2142/2044
24. https://www.researchgate.net
25. https://www.wto.org/english/tratop_e/devel_e/sem04_e/moreno.ppt
26. http://164.100.133.129:81/eCONTENT/Uploads/Electronic_Commerce.pdf
27. http://164.100.133.129:81/eCONTENT/Uploads/Electronic_Commerce.pdf
28. http://www.books.mec.biz/downloads/Electronic_Commerce/NDE2MzExOw
29. http://www.yorku.ca/dzwick/SP_Jain_02_Intro%20e-commerce.ppt
30. http://www.hkiaat.org/e-newsletter/Oct-14/technical_article/AAT8.pdf

31. http://steconomiceuoradea.ro/anale/volume/2006/economie-si-administrarea-afacerilor/42.pdf

32. https://www.internetsociety.org/sites/default/files/Brief_History_of_the_Internet.pdf

33. http://shodhganga.inflibnet.ac.in/bitstream/10603/113273/23/23_for%20further%20readings%20and%20research.pdf

34. http://janaushadhi.gov.in/data/Mobile%20Jan%20Aushadhi%20Store.pdf

35. http://janaushadhi.gov.in/data/Guidelines%20&%20Agreement%20for%20Individuals%20Sep,%202016.pdf

36. https://www.tutorialspoint.com/e_commerce/e_commerce_tutorial.pdf

37. http://www.ijettcs.org/Volume5Issue2/IJETTCS-2016-04-23-93.pdf

38. http://www.iracst.org/ijrmt/papers/vol6no32016/5vol6no3.pdf

39. https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf

40. http://webuser.hs-furtwangen.de/~heindl/ebte-08ss-law-in-business-Krishan.pdf

41. http://www.nasscom.in

42. http://www.emarketer.com/public_media/docs/eMarketer_eTailWest2016_Worldwide_ECommerce_Report.pdf

43. http://www.nielsen.com/content/dam/nielsenglobal/jp/docs/report/2016/Nielsen-Global-Connected-Commerce-Report-January-2016

44. http://www.criteo.com/media/3552/criteo-ecommerce-industry-outlook-2016.pdf

45. http://ethesis.nitrkl.ac.in/6738/1/Comparative__Gupta_2015.pdf

46. http://pezzottaitejournals.net/pezzottaite/images/ISSUES/V4N1/IJLSCMPV4N110.pdf

47. https://opus.lib.uts.edu.au/bitstream/10453/6945/1/2004003421.pdf

48. http://www.onlinejournal.in/IJIRV2I7/010.pdf

49. http://isrj.org/UploadedData/1144.pdf

50. http://www.criteo.com/media/4094/ovum-the-future-of-e-commerce-the-road-to-2026.pdf

51. http://www.scielo.cl/pdf/jtaer/v3n2/art03.pdftp://unctad.org/en/PublicationsLibrary/ier2015_en.pdf

52. https://www.divaportal.org/smash/get/diva2:121411/FULLTEXT01.pdf

53. http://ec.europa.eu/eurostat/documents/42577/3222224/Digital+economy+outlook+2015/dbdec3c6-ca38-432c-82f2-1e330d9d6a24

54. https://www.gov.uk

55. https://core.ac.uk/download/pdf/6313294.pdf

56. http://www.sciencedirect.com/science/article/pii/S0378720606001200

57. www.isrj.net "An Analytical Study Of E-commerce Growth In Developing Country Like India"

58. http://www.cengage.com/resource_uploads/downloads/061906269X_236713.pdf

59. http://steconomiceuoradea.ro/anale/volume/2006/economie-si-administrarea-afa

60. www.groundswell.fi/sim/academic/(sim)%20From%20B2C%20to%20C2C% 2

61. http://shodhganga.inflibnet.ac.in/bitstream/10603/113273/12/12_chapter%201.pdf

62. http://online-ecommerce-tips.blogspot.in/2010/06/4g2b-government-to-business.html

63. https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/

64. https://www.statista.com/topics/5054/cyber-crime-in-india/,

65. https://www.mygov.in/frontendgeneral/pdf/brief-on-misleading-advertisement.pdf

66. https://www.mygov.in/frontendgeneral/pdf/brief-on-misleading-advertisement.pdf

67. https://www.pocket-lint.com/apps/news/google/137722-what-is-google-assistant-how-does-it-work-and-which- devices-offer-it

68. ://www.moneycontrol.com

69. Influencer Marketing Hub, February 15th, 2020

70. https://datareportal.com/social-media-users

71. https://www.edibasics.com/what-is-edi/

72. https://www.trans-lex.org/450900/_/uncitral-model-law-on-international-commercial-arbitration/

73. http://www.uncitral.org/pdf/english/texts/electcom/05-89450 _Ebook.pdf

74. https://www.jus.uio.no/lm/un.arbitration.model.law.1985/7.

75. http://www.cch.ca/_resources/pdf/ecommerce_slides_url.pdf

76. http://www.egyankosh.ac.in

77. http:// www.antivirus.com

ANNEXURE

Annexure -1

रजिस्ट्री सं॰ डी॰ एल॰—(एन)04/0007/2003—19 REGISTERED NO. DL—(N)04/0007/2003—19

भारत का राजपत्र
The Gazette of India

असाधारण
EXTRAORDINARY
भाग II — खण्ड 1
PART II — Section 1
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं॰ 54] नई दिल्ली, शुक्रवार, अगस्त 9, 2019/ श्रावण 18, 1941 (शक)
No. 54] NEW DELHI, FRIDAY, AUGUST 9, 2019/SHRAVANA 18, 1941 (SAKA)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।
Separate paging is given to this Part in order that it may be filed as a separate compilation.

MINISTRY OF LAW AND JUSTICE
(Legislative Department)

New Delhi, the 9*th August,* 2019/*Shravana* 18, 1941 (*Saka*)

The following Act of Parliament received the assent of the President on the 9th August, 2019, and is hereby published for general information:—

THE CONSUMER PROTECTION ACT, 2019

No. 35 of 2019

[9*th August*, 2019.]

An Act to provide for protection of the interests of consumers and for the said purpose, to establish authorities for timely and effective administration and settlement of consumers' disputes and for matters connected therewith or incidental thereto.

Be it enacted by Parliament in the Seventieth Year of the Republic of India as follows:—

CHAPTER I

Preliminary

1. (*1*) This Act may be called the Consumer Protection Act, 2019. Short title, extent, commencement and application.

(*2*) It extends to the whole of India except the State of Jammu and Kashmir.

(*3*) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different States and for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

(*4*) Save as otherwise expressly provided by the Central Government, by notification, this Act shall apply to all goods and services.

Definitions.

2. In this Act, unless the context otherwise requires,—

(*1*) "advertisement" means any audio or visual publicity, representation, endorsement or pronouncement made by means of light, sound, smoke, gas, print, electronic media, internet or website and includes any notice, circular, label, wrapper, invoice or such other documents;

(*2*) "appropriate laboratory" means a laboratory or an organisation—

(*i*) recognised by the Central Government; or

(*ii*) recognised by a State Government, subject to such guidelines as may be issued by the Central Government in this behalf; or

(*iii*) established by or under any law for the time being in force, which is maintained, financed or aided by the Central Government or a State Government for carrying out analysis or test of any goods with a view to determining whether such goods suffer from any defect;

(*3*) "branch office" means—

(*i*) any office or place of work described as a branch by the establishment; or

(*ii*) any establishment carrying on either the same or substantially the same activity carried on by the head office of the establishment;

(*4*) "Central Authority" means the Central Consumer Protection Authority established under section 10;

(*5*) "complainant" means—

(*i*) a consumer; or

(*ii*) any voluntary consumer association registered under any law for the time being in force; or

(*iii*) the Central Government or any State Government; or

(*iv*) the Central Authority; or

(*v*) one or more consumers, where there are numerous consumers having the same interest; or

(*vi*) in case of death of a consumer, his legal heir or legal representative; or

(*vii*) in case of a consumer being a minor, his parent or legal guardian;

(*6*) "complaint" means any allegation in writing, made by a complainant for obtaining any relief provided by or under this Act, that—

(*i*) an unfair contract or unfair trade practice or a restrictive trade practice has been adopted by any trader or service provider;

(*ii*) the goods bought by him or agreed to be bought by him suffer from one or more defects;

(*iii*) the services hired or availed of or agreed to be hired or availed of by him suffer from any deficiency;

(*iv*) a trader or a service provider, as the case may be, has charged for the goods or for the services mentioned in the complaint, a price in excess of the price—

(*a*) fixed by or under any law for the time being in force; or (*b*) displayed on the goods or any package containing such goods; or

(*c*) displayed on the price list exhibited by him by or under any law for the time being in force; or

(*d*) agreed between the parties;

(*v*) the goods, which are hazardous to life and safety when used, are being offered for sale to the public—

(*a*) in contravention of standards relating to safety of such goods as required to be complied with, by or under any law for the time being in force;

(*b*) where the trader knows that the goods so offered are unsafe to the public;

(*vi*) the services which are hazardous or likely to be hazardous to life and safety of the public when used, are being offered by a person who provides any service and who knows it to be injurious to life and safety;

(*vii*) a claim for product liability action lies against the product manufacturer, product seller or product service provider, as the case may be;

(*7*) "consumer" means any person who—

(*i*) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment, when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose; or

(*ii*) hires or avails of any service for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such service other than the person who hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first mentioned person, but does not include a person who avails of such service for any commercial purpose.

Explanation.—For the purposes of this clause,—

(*a*) the expression "commercial purpose" does not include use by a person of goods bought and used by him exclusively for the purpose of earning his livelihood, by means of self-employment;

(*b*) the expressions "buys any goods" and "hires or avails any services" includes offline or online transactions through electronic means or by teleshopping or direct selling or multi-level marketing;

(*8*) "consumer dispute" means a dispute where the person against whom a complaint has been made, denies or disputes the allegations contained in the complaint;

(*9*) "consumer rights" includes,—

(*i*) the right to be protected against the marketing of goods, products or services which are hazardous to life and property;

(*ii*) the right to be informed about the quality, quantity, potency, purity, standard and price of goods, products or services, as the case may be, so as to protect the consumer against unfair trade practices;

(*iii*) the right to be assured, wherever possible, access to a variety of goods, products or services at competitive prices;

(*iv*) the right to be heard and to be assured that consumer's interests will receive due consideration at appropriate fora;

(*v*) the right to seek redressal against unfair trade practice or restrictive trade practices or unscrupulous exploitation of consumers; and

(*vi*) the right to consumer awareness;

(*10*) "defect" means any fault, imperfection or shortcoming in the quality, quantity, potency, purity or standard which is required to be maintained by or under any law for the time being in force or under any contract, express or implied or as is claimed by the trader in any manner whatsoever in relation to any goods or product and the expression "defective" shall be construed accordingly;

(*11*) "deficiency" means any fault, imperfection, shortcoming or inadequacy in the quality, nature and manner of performance which is required to be maintained by or under any law for the time being in force or has been undertaken to be performed by a person in pursuance of a contract or otherwise in relation to any service and includes—

(*i*) any act of negligence or omission or commission by such person which causes loss or injury to the consumer; and

(*ii*) deliberate withholding of relevant information by such person to the consumer;

(*12*) "design", in relation to a product, means the intended or known physical and material characteristics of such product and includes any intended or known formulation or content of such product and the usual result of the intended manufacturing or other process used to produce such product;

(*13*) "direct selling" means marketing, distribution and sale of goods or provision of services through a network of sellers, other than through a permanent retail location;

(*14*) "Director-General" means the Director-General appointed under sub-section (*2*) of section 15;

(*15*) "District Commission" means a District Consumer Disputes Redressal Commission established under sub-section (*1*) of section 28;

(*16*) "e-commerce" means buying or selling of goods or services including digital products over digital or electronic network;

(*17*) "electronic service provider" means a person who provides technologies or processes to enable a product seller to engage in advertising or selling goods or services to a consumer and includes any online market place or online auction sites;

(*18*) "endorsement", in relation to an advertisement, means—

(*i*) any message, verbal statement, demonstration; or

(*ii*) depiction of the name, signature, likeness or other identifiable personal characteristics of an individual; or

(*iii*) depiction of the name or seal of any institution or organisation,

which makes the consumer to believe that it reflects the opinion, finding or experience of the person making such endorsement;

(*19*) "establishment" includes an advertising agency, commission agent, manufacturing, trading or any other commercial agency which carries on any business, trade or profession or any work in connection with or incidental or ancillary to any commercial activity, trade or profession, or such other class or classes of persons including public utility entities in the manner as may be prescribed;

(*20*) "express warranty" means any material statement, affirmation of fact, promise or description relating to a product or service warranting that it conforms to such material statement, affirmation, promise or description and includes any sample or model of a product warranting that the whole of such product conforms to such sample or model;

(*21*) "goods" means every kind of movable property and includes "food" as defined in clause (*j*) of sub-section (*1*) of section 3 of the Food Safety and Standards Act, 2006;

34 of 2006.

(*22*) "harm", in relation to a product liability, includes—

(*i*) damage to any property, other than the product itself;

(*ii*) personal injury, illness or death;

(*iii*) mental agony or emotional distress attendant to personal injury or illness or damage to property; or

(*iv*) any loss of consortium or services or other loss resulting from a harm referred to in sub-clause (*i*) or sub-clause (*ii*) or sub-clause (*iii*),

but shall not include any harm caused to a product itself or any damage to the property on account of breach of warranty conditions or any commercial or economic loss, including any direct, incidental or consequential loss relating thereto;

(*23*) "injury" means any harm whatever illegally caused to any person, in body, mind or property;

(*24*) "manufacturer" means a person who—

(*i*) makes any goods or parts thereof; or

(*ii*) assembles any goods or parts thereof made by others; or

(*iii*) puts or causes to be put his own mark on any goods made by any other person;

(*25*) "mediation" means the process by which a mediator mediates the consumer disputes;

(*26*) "mediator" means a mediator referred to in section 75;

(*27*) "member" includes the President and a member of the National Commission or a State Commission or a District Commission, as the case may be;

(*28*) "misleading advertisement" in relation to any product or service, means an advertisement, which—

(*i*) falsely describes such product or service; or

(*ii*) gives a false guarantee to, or is likely to mislead the consumers as to the nature, substance, quantity or quality of such product or service; or

(*iii*) conveys an express or implied representation which, if made by the manufacturer or seller or service provider thereof, would constitute an unfair trade practice; or

(*iv*) deliberately conceals important information;

(*29*) "National Commission" means the National Consumer Disputes Redressal Commission established under sub-section (*1*) of section 53;

(*30*) "notification" means a notification published in the Official Gazette and the term "notify" shall be construed accordingly;

(*31*) "person" includes—

(*i*) an individual;

(*ii*) a firm whether registered or not;

(*iii*) a Hindu undivided family;

(*iv*) a co-operative society;

(*v*) an association of persons whether registered under the Societies Registration Act, 1860 or not; 21 of 1860.

(*vi*) any corporation, company or a body of individuals whether incorporated or not;

(*vii*) any artificial juridical person, not falling within any of the preceding sub-clauses;

(*32*) "prescribed" means prescribed by rules made by the Central Government, or, as the case may be, the State Government;

(*33*) "product" means any article or goods or substance or raw material or any extended cycle of such product, which may be in gaseous, liquid, or solid state possessing intrinsic value which is capable of delivery either as wholly assembled or as a component part and is produced for introduction to trade or commerce, but does not include human tissues, blood, blood products and organs;

(*34*) "product liability" means the responsibility of a product manufacturer or product seller, of any product or service, to compensate for any harm caused to a consumer by such defective product manufactured or sold or by deficiency in services relating thereto;

(*35*) "product liability action" means a complaint filed by a person before a District Commission or State Commission or National Commission, as the case may be, for claiming compensation for the harm caused to him;

(*36*) "product manufacturer" means a person who—

(*i*) makes any product or parts thereof; or

(*ii*) assembles parts thereof made by others; or

(*iii*) puts or causes to be put his own mark on any products made by any other person; or

(*iv*) makes a product and sells, distributes, leases, installs, prepares, packages, labels, markets, repairs, maintains such product or is otherwise involved in placing such product for commercial purpose; or

(*v*) designs, produces, fabricates, constructs or re-manufactures any product before its sale; or

(*vi*) being a product seller of a product, is also a manufacturer of such product;

(*37*) "product seller", in relation to a product, means a person who, in the course of business, imports, sells, distributes, leases, installs, prepares, packages, labels, markets, repairs, maintains, or otherwise is involved in placing such product for commercial purpose and includes—

(*i*) a manufacturer who is also a product seller; or (*ii*) a service provider,

but does not include—

(*a*) a seller of immovable property, unless such person is engaged in the sale of constructed house or in the construction of homes or flats;

(*b*) a provider of professional services in any transaction in which, the sale or use of a product is only incidental thereto, but furnishing of opinion, skill or services being the essence of such transaction;

(*c*) a person who—

(*I*) acts only in a financial capacity with respect to the sale of the product;

(*II*) is not a manufacturer, wholesaler, distributor, retailer, direct seller or an electronic service provider;

(*III*) leases a product, without having a reasonable opportunity to inspect and discover defects in the product, under a lease arrangement in which the selection, possession, maintenance, and operation of the product are controlled by a person other than the lessor;

(*38*) "product service provider", in relation to a product, means a person who provides any service in respect of such product;

(*39*) "regulations" means the regulations made by the National Commission, or as the case may be, the Central Authority;

(*40*) "Regulator" means a body or any authority established under any other law for the time being in force;

(*41*) "restrictive trade practice" means a trade practice which tends to bring about manipulation of price or its conditions of delivery or to affect flow of supplies in the market relating to goods or services in such a manner as to impose on the consumers unjustified costs or restrictions and shall include—

(*i*) delay beyond the period agreed to by a trader in supply of such goods or in providing the services which has led or is likely to lead to rise in the price;

(*ii*) any trade practice which requires a consumer to buy, hire or avail of any goods or, as the case may be, services as condition precedent for buying, hiring or availing of other goods or services;

(*42*) "service" means service of any description which is made available to potential users and includes, but not limited to, the provision of facilities in connection with banking, financing, insurance, transport, processing, supply of electrical or other energy, telecom, boarding or lodging or both, housing construction, entertainment, amusement or the purveying of news or other information, but does not include the rendering of any service free of charge or under a contract of personal service;

(*43*) "spurious goods" means such goods which are falsely claimed to be genuine;

(*44*) "State Commission" means a State Consumer Disputes Redressal Commission established under sub-section (*1*) of section 42;

(*45*) "trader", in relation to any goods, means a person who sells or distributes any goods for sale and includes the manufacturer thereof, and where such goods are sold or distributed in package form, includes the packer thereof;

(*46*) "unfair contract" means a contract between a manufacturer or trader or service provider on one hand, and a consumer on the other, having such terms which cause significant change in the rights of such consumer, including the following, namely:—

(*i*) requiring manifestly excessive security deposits to be given by a consumer for the performance of contractual obligations; or

(*ii*) imposing any penalty on the consumer, for the breach of contract thereof which is wholly disproportionate to the loss occurred due to such breach to the other party to the contract; or

(*iii*) refusing to accept early repayment of debts on payment of applicable penalty; or

(*iv*) entitling a party to the contract to terminate such contract unilaterally, without reasonable cause; or

(*v*) permitting or has the effect of permitting one party to assign the contract to the detriment of the other party who is a consumer, without his consent; or

(*vi*) imposing on the consumer any unreasonable charge, obligation or condition which puts such consumer to disadvantage;

(*47*) "unfair trade practice" means a trade practice which, for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive practice including any of the following practices, namely:—

(*i*) making any statement, whether orally or in writing or by visible representation including by means of electronic record, which—

(*a*) falsely represents that the goods are of a particular standard, quality, quantity, grade, composition, style or model;

(*b*) falsely represents that the services are of a particular standard, quality or grade;

(*c*) falsely represents any re-built, second-hand, renovated, reconditioned or old goods as new goods;

(*d*) represents that the goods or services have sponsorship, approval, performance, characteristics, accessories, uses or benefits which such goods or services do not have;

(*e*) represents that the seller or the supplier has a sponsorship or approval or affiliation which such seller or supplier does not have;

(*f*) makes a false or misleading representation concerning the need for, or the usefulness of, any goods or services;

(*g*) gives to the public any warranty or guarantee of the performance, efficacy or length of life of a product or of any goods that is not based on an adequate or proper test thereof:

Provided that where a defence is raised to the effect that such warranty or guarantee is based on adequate or proper test, the burden of proof of such defence shall lie on the person raising such defence;

(*h*) makes to the public a representation in a form that purports to be—

(*A*) a warranty or guarantee of a product or of any goods or services; or

(*B*) a promise to replace, maintain or repair an article or any part thereof or to repeat or continue a service until it has achieved a specified result, if such purported warranty or guarantee or promise is materially misleading or if there is no reasonable prospect that such warranty, guarantee or promise will be carried out;

(*i*) materially misleads the public concerning the price at which a product or like products or goods or services, have been or are, ordinarily sold or provided, and, for this purpose, a representation as to price shall be deemed to refer to the price at which the product or goods or services has or have been sold by sellers or provided by suppliers generally in the relevant market unless it is clearly specified to be the price at which the product has been sold or services have been provided by the person by whom or on whose behalf the representation is made;

(*j*) gives false or misleading facts disparaging the goods, services or trade of another person.

Explanation.—For the purposes of this sub-clause, a statement that is,—

(*A*) expressed on an article offered or displayed for sale, or on its wrapper or container; or

(*B*) expressed on anything attached to, inserted in, or accompanying, an article offered or displayed for sale, or on anything on which the article is mounted for display or sale; or

(*C*) contained in or on anything that is sold, sent, delivered, transmitted or in any other manner whatsoever made available to a member of the public,

shall be deemed to be a statement made to the public by, and only by, the person who had caused the statement to be so expressed, made or contained;

(*ii*) permitting the publication of any advertisement, whether in any newspaper or otherwise, including by way of electronic record, for the sale or supply at a bargain price of goods or services that are not intended to be offered for sale or supply at the bargain price, or for a period that is, and in quantities that are, reasonable, having regard to the nature of the market in which the business is carried on, the nature and size of business, and the nature of the advertisement.

Explanation.—For the purpose of this sub-clause, "bargain price" means,—

(*A*) a price that is stated in any advertisement to be a bargain price, by reference to an ordinary price or otherwise; or

(*B*) a price that a person who reads, hears or sees the advertisement, would reasonably understand to be a bargain price having regard to the prices at which the product advertised or like products are ordinarily sold;

(*iii*) permitting—

(*a*) the offering of gifts, prizes or other items with the intention of not providing them as offered or creating impression that something is being given or offered free of charge when it is fully or partly covered by the amount charged, in the transaction as a whole;

(*b*) the conduct of any contest, lottery, game of chance or skill, for the purpose of promoting, directly or indirectly, the sale, use or supply of any product or any business interest, except such contest, lottery, game of chance or skill as may be prescribed;

(*c*) withholding from the participants of any scheme offering gifts, prizes or other items free of charge on its closure, the information about final results of the scheme.

Explanation.—For the purpose of this sub-clause, the participants of a scheme shall be deemed to have been informed of the final results of the scheme where such results are within a reasonable time published, prominently in the same newspaper in which the scheme was originally advertised;

(*iv*) permitting the sale or supply of goods intended to be used, or are of a kind likely to be used by consumers, knowing or having reason to believe that the goods do not comply with the standards prescribed by the competent authority relating to performance, composition, contents, design, constructions, finishing or packaging as are necessary to prevent or reduce the risk of injury to the person using the goods;

(*v*) permitting the hoarding or destruction of goods, or refusal to sell the goods or to make them available for sale or to provide any service, if such hoarding or destruction or refusal raises or tends to raise or is intended to raise, the cost of those or other similar goods or services;

(*vi*) manufacturing of spurious goods or offering such goods for sale or adopting deceptive practices in the provision of services;

(*vii*) not issuing bill or cash memo or receipt for the goods sold or services rendered in such manner as may be prescribed;

(*viii*) refusing, after selling goods or rendering services, to take back or withdraw defective goods or to withdraw or discontinue deficient services and to refund the consideration thereof, if paid, within the period stipulated in the bill or cash memo or receipt or in the absence of such stipulation, within a period of thirty days;

(*ix*) disclosing to other person any personal information given in confidence by the consumer unless such disclosure is made in accordance with the provisions of any law for the time being in force.

CHAPTER II

CONSUMER PROTECTION COUNCILS

Central Consumer Protection Council.

3. (*1*) The Central Government shall, by notification, establish with effect from such date as it may specify in that notification, the Central Consumer Protection Council to be known as the Central Council.

(*2*) The Central Council shall be an advisory council and consist of the following members, namely:—

(*a*) the Minister-in-charge of the Department of Consumer Affairs in the Central Government, who shall be the Chairperson; and

(*b*) such number of other official or non-official members representing such interests as may be prescribed.

Procedure for meetings of Central Council.

4. (*1*) The Central Council shall meet as and when necessary, but at least one meeting of the Council shall be held every year.

(*2*) The Central Council shall meet at such time and place as the Chairperson may think fit and shall observe such procedure in regard to the transaction of its business as may be prescribed.

Objects of Central Council.

5. The objects of the Central Council shall be to render advice on promotion and protection of the consumers' rights under this Act.

State Consumer Protection Councils.

6. (*1*) Every State Government shall, by notification, establish with effect from such date as it may specify in such notification, a State Consumer Protection Council for such State to be known as the State Council.

(*2*) The State Council shall be an advisory council and consist of the following members, namely:—

(*a*) the Minister-in-charge of Consumer Affairs in the State Government who shall be the Chairperson;

(*b*) such number of other official or non-official members representing such interests as may be prescribed;

(*c*) such number of other official or non-official members, not exceeding ten, as may be nominated by the Central Government.

(*3*) The State Council shall meet as and when necessary but not less than two meetings shall be held every year.

(*4*) The State Council shall meet at such time and place as the Chairperson may think fit and shall observe such procedure in regard to the transaction of its business, as may be prescribed.

Objects of State Council.

7. The objects of every State Council shall be to render advice on promotion and protection of consumer rights under this Act within the State.

District Consumer Protection Council.

8. (*1*) The State Government shall, by notification, establish for every District with effect from such date as it may specify in such notification, a District Consumer Protection Council to be known as the District Council.

(*2*) The District Council shall be an advisory council and consist of the following members, namely:—

(*a*) the Collector of the district (by whatever name called), who shall be the Chairperson; and

(*b*) such number of other official and non-official members representing such interests as may be prescribed.

(*3*) The District Council shall meet as and when necessary but not less than two meetings shall be held every year.

(*4*) The District Council shall meet at such time and place within the district as the Chairperson may think fit and shall observe such procedure in regard to the transaction of its business as may be prescribed.

Objects of District Council.

9. The objects of every District Council shall be to render advice on promotion and protection of consumer rights under this Act within the district.

CHAPTER III

CENTRAL CONSUMER PROTECTION AUTHORITY

Establishment of Central Consumer Protection Authority.

10. (*1*) The Central Government shall, by notification, establish with effect from such date as it may specify in that notification, a Central Consumer Protection Authority to be known as the Central Authority to regulate matters relating to violation of rights of consumers, unfair trade practices and false or misleading advertisements which are prejudicial to the interests of public and consumers and to promote, protect and enforce the rights of consumers as a class.

(*2*) The Central Authority shall consist of a Chief Commissioner and such number of other Commissioners as may be prescribed, to be appointed by the Central Government to exercise the powers and discharge the functions under this Act.

(*3*) The headquarters of the Central Authority shall be at such place in the National Capital Region of Delhi, and it shall have regional and other offices in any other place in India as the Central Government may decide.

Qualifications, method of recruitment, etc., of Chief Commissioner and Commissioners.

11. The Central Government may, by notification, make rules to provide for the qualifications for appointment, method of recruitment, procedure for appointment, term of office, salaries and allowances, resignation, removal and other terms and conditions of the service of the Chief Commissioner and Commissioners of the Central Authority.

Vacancy, etc., not to invalidate proceedings of Central Authority.

12. No act or proceeding of the Central Authority shall be invalid merely by reason of—

(*a*) any vacancy in, or any defect in the constitution of, the Central Authority; or

(*b*) any defect in the appointment of a person acting as the Chief Commissioner or as a Commissioner; or

(*c*) any irregularity in the procedure of the Central Authority not affecting the merits of the case.

Appointment of officers, experts, professionals and other employees of Central Authority.

13. (*1*) The Central Government shall provide the Central Authority such number of officers and other employees as it considers necessary for the efficient performance of its functions under this Act.

(2) The salaries and allowances payable to, and the other terms and conditions of service of, the officers and other employees of the Central Authority appointed under this Act shall be such as may be prescribed.

(*3*) The Central Authority may engage, in accordance with the procedure specified by regulations, such number of experts and professionals of integrity and ability, who have special knowledge and experience in the areas of consumer rights and welfare, consumer policy, law, medicine, food safety, health, engineering, product safety, commerce, economics, public affairs or administration, as it deems necessary to assist it in the discharge of its functions under this Act.

Procedure of Central Authority.

14. (*1*) The Central Authority shall regulate the procedure for transaction of its business and allocation of its business amongst the Chief Commissioner and Commissioners as may be specified by regulations.

(*2*) The Chief Commissioner shall have the powers of general superintendence, direction and control in respect of all administrative matters of the Central Authority:

Provided that the Chief Commissioner may delegate such of his powers relating to administrative matters of the Central Authority, as he may think fit, to any Commissioner (including Commissioner of a regional office) or any other officer of the Central Authority.

Investigation Wing.

15. (*1*) The Central Authority shall have an Investigation Wing headed by a Director-General for the purpose of conducting inquiry or investigation under this Act as may be directed by the Central Authority.

(*2*) The Central Government may appoint a Director-General and such number of Additional Director-General, Director, Joint Director, Deputy Director and Assistant Director, from amongst persons who have experience in investigation and possess such qualifications, in such manner, as may be prescribed.

(*3*) Every Additional Director-General, Director, Joint Director, Deputy Director and Assistant Director shall exercise his powers, and discharge his functions, subject to the general control, supervision and direction of the Director-General.

(*4*) The Director-General may delegate all or any of his powers to the Additional Director-General or Director, Joint Director or Deputy Director or Assistant Director, as the case may be, while conducting inquiries or investigations under this Act.

(*5*) The inquiries or the investigations made by the Director- General shall be submitted to the Central Authority in such form, in such manner and within such time, as may be specified by regulations.

Power of District Collector.

16. The District Collector (by whatever name called) may, on a complaint or on a reference made to him by the Central Authority or the Commissioner of a regional office, inquire into or investigate complaints regarding violation of rights of consumers as a class, on matters relating to violations of consumer rights, unfair trade practices and false or misleading advertisements, within his jurisdiction and submit his report to the Central Authority or to the Commissioner of a regional office, as the case may be.

Complaints to authorities.

17. A complaint relating to violation of consumer rights or unfair trade practices or false or misleading advertisements which are prejudicial to the interests of consumers as a class, may be forwarded either in writing or in electronic mode, to any one of the authorities, namely, the District Collector or the Commissioner of regional office or the Central Authority.

Powers and functions of Central Authority.

18. (*1*) The Central Authority shall—

(*a*) protect, promote and enforce the rights of consumers as a class, and prevent violation of consumers rights under this Act;

(*b*) prevent unfair trade practices and ensure that no person engages himself in unfair trade practices;

(*c*) ensure that no false or misleading advertisement is made of any goods or services which contravenes the provisions of this Act or the rules or regulations made thereunder;

(*d*) ensure that no person takes part in the publication of any advertisement which is false or misleading.

(*2*) Without prejudice to the generality of the provisions contained in sub-section (*1*), the Central Authority may, for any of the purposes aforesaid,—

(*a*) inquire or cause an inquiry or investigation to be made into violations of consumer rights or unfair trade practices, either *suo motu* or on a complaint received or on the directions from the Central Government;

(*b*) file complaints before the District Commission, the State Commission or the National Commission, as the case may be, under this Act;

(*c*) intervene in any proceedings before the District Commission or the State Commission or the National Commission, as the case may be, in respect of any allegation of violation of consumer rights or unfair trade practices;

(*d*) review the matters relating to, and the factors inhibiting enjoyment of, consumer rights, including safeguards provided for the protection of consumers under any other law for the time being in force and recommend appropriate remedial measures for their effective implementation;

(*e*) recommend adoption of international covenants and best international practices on consumer rights to ensure effective enforcement of consumer rights;

(*f*) undertake and promote research in the field of consumer rights;

(*g*) spread and promote awareness on consumer rights;

(*h*) encourage non-Governmental organisations and other institutions working in the field of consumer rights to co-operate and work with consumer protection agencies;

(*i*) mandate the use of unique and universal goods identifiers in such goods, as may be necessary, to prevent unfair trade practices and to protect consumers' interest;

(*j*) issue safety notices to alert consumers against dangerous or hazardous or unsafe goods or services;

(*k*) advise the Ministries and Departments of the Central and State Governments on consumer welfare measures;

(*l*) issue necessary guidelines to prevent unfair trade practices and protect consumers' interest.

Power of Central Authority to refer matter for investigation or to other Regulator.

19. (*1*) The Central Authority may, after receiving any information or complaint or directions from the Central Government or of its own motion, conduct or cause to be conducted a preliminary inquiry as to whether there exists a *prima facie* case of violation of consumer rights or any unfair trade practice or any false or misleading advertisement, by any person, which is prejudicial to the public interest or to the interests of consumers and if it is satisfied that there exists a *prima facie* case, it shall cause investigation to be made by the Director-General or by the District Collector.

(*2*) Where, after preliminary inquiry, the Central Authority is of the opinion that the matter is to be dealt with by a Regulator established under any other law for the time being in force, it may refer such matter to the concerned Regulator along with its report.

(*3*) For the purposes of investigation under sub-section (*1*), the Central Authority, the Director General or the District Collector may call upon a person referred to in sub-section (*1*) and also direct him to produce any document or record in his possession.

Power of Central Authority to recall goods, etc.

20. Where the Central Authority is satisfied on the basis of investigation that there is sufficient evidence to show violation of consumer rights or unfair trade practice by a person, it may pass such order as may be necessary, including—

(*a*) recalling of goods or withdrawal of services which are dangerous, hazardous or unsafe;

(*b*) reimbursement of the prices of goods or services so recalled to purchasers of such goods or services; and

(*c*) discontinuation of practices which are unfair and prejudicial to consumers' interest:

Provided that the Central Authority shall give the person an opportunity of being heard before passing an order under this section.

Power of Central Authority to issue directions and penalties against false or misleading advertisements.

21. (*1*) Where the Central Authority is satisfied after investigation that any advertisement is false or misleading and is prejudicial to the interest of any consumer or is in contravention of consumer rights, it may, by order, issue directions to the concerned trader or manufacturer or endorser or advertiser or publisher, as the case may be, to discontinue such advertisement or to modify the same in such manner and within such time as may be specified in that order.

(*2*) Notwithstanding the order passed under sub-section (*1*), if the Central Authority is of the opinion that it is necessary to impose a penalty in respect of such false or misleading advertisement, by a manufacturer or an endorser, it may, by order, impose on manufacturer or endorser a penalty which may extend to ten lakh rupees:

Provided that the Central Authority may, for every subsequent contravention by a manufacturer or endorser, impose a penalty, which may extend to fifty lakh rupees.

(*3*) Notwithstanding any order under sub-sections (*1*) and (*2*), where the Central Authority deems it necessary, it may, by order, prohibit the endorser of a false or misleading advertisement from making endorsement of any product or service for a period which may extend to one year:

Provided that the Central Authority may, for every subsequent contravention, prohibit such endorser from making endorsement in respect of any product or service for a period which may extend to three years.

(*4*) Where the Central Authority is satisfied after investigation that any person is found to publish, or is a party to the publication of, a misleading advertisement, it may impose on such person a penalty which may extend to ten lakh rupees.

(*5*) No endorser shall be liable to a penalty under sub-sections (*2*) and (*3*) if he has exercised due diligence to verify the veracity of the claims made in the advertisement regarding the product or service being endorsed by him.

(*6*) No person shall be liable to such penalty if he proves that he had published or arranged for the publication of such advertisement in the ordinary course of his business:

Provided that no such defence shall be available to such person if he had previous knowledge of the order passed by the Central Authority for withdrawal or modification of such advertisement.

(*7*) While determining the penalty under this section, regard shall be had to the following, namely:—

(*a*) the population and the area impacted or affected by such offence;

(*b*) the frequency and duration of such offence;

(*c*) the vulnerability of the class of persons likely to be adversely affected by such offence; and

(*d*) the gross revenue from the sales effected by virtue of such offence.

(*8*) The Central Authority shall give the person an opportunity of being heard before an order under this section is passed.

Search and seizure.

22. (*1*) For the purpose of conducting an investigation after preliminary inquiry under sub-section (*1*) of section 19, the Director-General or any other officer authorised by him in this behalf, or the District Collector, as the case may be, may, if he has any reason to believe that any person has violated any consumer rights or committed unfair trade practice or causes any false or misleading advertisement to be made, shall,—

(*a*) enter at any reasonable time into any such premises and search for any document or record or article or any other form of evidence and seize such document, record, article or such evidence;

(*b*) make a note or an inventory of such record or article; or

(*c*) require any person to produce any record, register or other document or article.

2 of 1974. (*2*) The provisions of the Code of Criminal Procedure, 1973, relating to search and seizure shall apply, as far as may be, for search and seizure under this Act.

(*3*) Every document, record or article seized under clause (*a*) of sub-section (*1*) or produced under clause (*c*) of that sub-section shall be returned to the person, from whom they were seized or who produced the same, within a period of twenty days of the date of such seizure or production, as the case may be, after copies thereof or extracts therefrom certified by that person, in such manner as may be prescribed, have been taken.

(*4*) Where any article seized under sub-section (*1*) are subject to speedy or natural decay, the Director-General or such other officer may dispose of the article in such manner as may be prescribed.

(*5*) In the case of articles other than the articles referred to in sub-section (*4*), provisions contained in clause (*c*) of sub-section (*2*) of section 38 shall *mutatis mutandis* apply in relation to analysis or tests.

Designation of any statutory authority or body to function as Central Authority.

23. The Central Government may, if it considers necessary, by notification, designate any statutory authority or body to exercise the powers and perform the functions of the Central Authority referred to in section 10.

Appeal.

24. A person aggrieved by any order passed by the Central Authority under sections 20 and 21 may file an appeal to the National Commission within a period of thirty days from the date of receipt of such order.

Grants by Central Government.

25. The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Central Authority grants of such sums of money as that Government may think fit for being utilised for the purposes of this Act.

Accounts and audit.

26. (*1*) The Central Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form and manner as may be prescribed in consultation with the Comptroller and Auditor-General of India.

(*2*) The accounts of the Central Authority shall be audited by the Comptroller and Auditor-General of India at such intervals as may be specified by him and any expenditure incurred in connection with such audit shall be payable by the Central Authority to the Comptroller and Auditor-General of India.

(*3*) The Comptroller and Auditor-General of India or any other person appointed by him in connection with the audit of the accounts of the Central Authority shall have the same rights, privileges and authority in connection with such audit as the Comptroller and Auditor-General of India generally has, in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of books, accounts, connected vouchers and other documents and papers and to inspect any of the offices of the Central Authority.

(*4*) The accounts of the Central Authority as certified by the Comptroller and Auditor-General of India or any other person appointed by him in this behalf together with the audit report thereon shall be forwarded annually to the Central Government which shall cause the same to be laid before each House of Parliament.

Furnishing of annual reports, etc.

27. (*1*) The Central Authority shall prepare once in every year, in such form, manner and at such time as may be prescribed, an annual report giving full account of its activities during the previous year and such other reports and returns, as may be directed, and copies of such report and returns shall be forwarded to the Central Government.

(*2*) A copy of the annual report received under sub-section (*1*) shall be laid, as soon as may be after it is received, before each House of Parliament.

CHAPTER IV

CONSUMER DISPUTES REDRESSAL COMMISSION

Establishment of District Consumer Disputes Redressal Commission.

28. (*1*) The State Government shall, by notification, establish a District Consumer Disputes Redressal Commission, to be known as the District Commission, in each district of the State:

Provided that the State Government may, if it deems fit, establish more than one District Commission in a district.

(*2*) Each District Commission shall consist of—

(*a*) a President; and

(*b*) not less than two and not more than such number of members as may be prescribed, in consultation with the Central Government.

29. The Central Government may, by notification, make rules to provide for the qualifications, method of recruitment, procedure for appointment, term of office, resignation and removal of the President and members of the District Commission.

Qualifications, etc., of President and members of District Commission.

30. The State Government may, by notification, make rules to provide for salaries and allowances and other terms and conditions of service of the President, and members of the District Commission.

Salaries, allowances and other terms and conditions of service of President and members of District Commission.

31. Any person appointed as President or, as the case may be, a member of the District Commission immediately before the commencement of this Act shall hold office as such as President or, as the case may be, as member till the completion of his term for which he has been appointed.

Transitional provision.

32. If, at any time, there is a vacancy in the office of the President or member of a District Commission, the State Government may, by notification, direct—

Vacancy in office of member of District Commission.

(*a*) any other District Commission specified in that notification to exercise the jurisdiction in respect of that district also; or

(*b*) the President or a member of any other District Commission specified in that notification to exercise the powers and discharge the functions of the President or member of that District Commission also.

33. (*1*) The State Government shall provide the District Commission with such officers and other employees as may be required to assist the District Commission in the discharge of its functions.

Officers and other employees of District Commission.

(*2*) The officers and other employees of the District Commission shall discharge their functions under the general superintendence of the President of the District Commission.

(*3*) The salaries and allowances payable to, and the other terms and conditions of service of, the officers and other employees of the District Commission shall be such as may be prescribed.

34. (*1*) Subject to the other provisions of this Act, the District Commission shall have jurisdiction to entertain complaints where the value of the goods or services paid as consideration does not exceed one crore rupees:

Jurisdiction of District Commission.

Provided that where the Central Government deems it necessary so to do, it may prescribe such other value, as it deems fit.

(*2*) A complaint shall be instituted in a District Commission within the local limits of whose jurisdiction,—

(*a*) the opposite party or each of the opposite parties, where there are more than one, at the time of the institution of the complaint, ordinarily resides or carries on business or has a branch office or personally works for gain; or

(*b*) any of the opposite parties, where there are more than one, at the time of the institution of the complaint, actually and voluntarily resides, or carries on business or has a branch office, or personally works for gain, provided that in such case the permission of the District Commission is given; or

(*c*) the cause of action, wholly or in part, arises; or

(*d*) the complainant resides or personally works for gain.

(*3*) The District Commission shall ordinarily function in the district headquarters and may perform its functions at such other place in the district, as the State Government may, in consultation with the State Commission, notify in the Official Gazette from time to time.

Manner in which complaint shall be made.

35. (*1*) A complaint, in relation to any goods sold or delivered or agreed to be sold or delivered or any service provided or agreed to be provided, may be filed with a District Commission by—

(*a*) the consumer,—

(*i*) to whom such goods are sold or delivered or agreed to be sold or delivered or such service is provided or agreed to be provided; or

(*ii*) who alleges unfair trade practice in respect of such goods or service;

(*b*) any recognised consumer association, whether the consumer to whom such goods are sold or delivered or agreed to be sold or delivered or such service is provided or agreed to be provided, or who alleges unfair trade practice in respect of such goods or service, is a member of such association or not;

(*c*) one or more consumers, where there are numerous consumers having the same interest, with the permission of the District Commission, on behalf of, or for the benefit of, all consumers so interested; or

(*d*) the Central Government, the Central Authority or the State Government, as the case may be:

Provided that the complaint under this sub-section may be filed electronically in such manner as may be prescribed.

Explanation.—For the purposes of this sub-section, "recognised consumer association" means any voluntary consumer association registered under any law for the time being in force.

(*2*) Every complaint filed under sub-section (*1*) shall be accompanied with such fee and payable in such manner, including electronic form, as may be prescribed.

Proceedings before District Commission.

36. (*1*) Every proceeding before the District Commission shall be conducted by the President of that Commission and atleast one member thereof, sitting together:

Provided that where a member, for any reason, is unable to conduct a proceeding till it is completed, the President and the other member shall continue the proceeding from the stage at which it was last heard by the previous member.

(*2*) On receipt of a complaint made under section 35, the District Commission may, by order, admit the complaint for being proceeded with or reject the same:

Provided that a complaint shall not be rejected under this section unless an opportunity of being heard has been given to the complainant:

Provided further that the admissibility of the complaint shall ordinarily be decided within twenty-one days from the date on which the complaint was filed.

(*3*) Where the District Commission does not decide the issue of admissibility of the complaint within the period so specified, it shall be deemed to have been admitted.

Reference to mediation.

37. (*1*) At the first hearing of the complaint after its admission, or at any later stage, if it appears to the District Commission that there exists elements of a settlement which may be acceptable to the parties, except in such cases as may be prescribed, it may direct the parties to give in writing, within five days, consent to have their dispute settled by mediation in accordance with the provisions of Chapter V.

(*2*) Where the parties agree for settlement by mediation and give their consent in writing, the District Commission shall, within five days of receipt of such consent, refer the matter for mediation, and in such case, the provisions of Chapter V, relating to mediation, shall apply.

Procedure on admission of complaint.

38. (*1*) The District Commission shall, on admission of a complaint, or in respect of cases referred for mediation on failure of settlement by mediation, proceed with such complaint.

(*2*) Where the complaint relates to any goods, the District Commission shall,—

(*a*) refer a copy of the admitted complaint, within twenty-one days from the date of its admission to the opposite party mentioned in the complaint directing him to give his version of the case within a period of thirty days or such extended period not exceeding fifteen days as may be granted by it;

(*b*) if the opposite party on receipt of a complaint referred to him under clause (*a*) denies or disputes the allegations contained in the complaint, or omits or fails to take any action to represent his case within the time given by the District Commission, proceed to settle the consumer dispute in the manner specified in clauses (*c*) to (*g*);

(*c*) if the complaint alleges a defect in the goods which cannot be determined without proper analysis or test of the goods, obtain a sample of the goods from the complainant, seal it and authenticate it in the manner as may be prescribed and refer the sample so sealed to the appropriate laboratory along with a direction that such laboratory to make an analysis or test, whichever may be necessary, with a view to finding out whether such goods suffer from any defect alleged in the complaint or from any other defect and to report its findings thereon to the District Commission within a period of forty-five days of the receipt of the reference or within such extended period as may be granted by it;

(*d*) before any sample of the goods is referred to any appropriate laboratory under clause (*c*), require the complainant to deposit to the credit of the Commission such fees as may be specified, for payment to the appropriate laboratory for carrying out the necessary analysis or test in relation to the goods in question;

(*e*) remit the amount deposited to its credit under clause (*d*) to the appropriate laboratory to enable it to carry out the analysis or test mentioned in clause (*c*) and on receipt of the report from the appropriate laboratory, it shall forward a copy of the report along with such remarks as it may feel appropriate to the opposite party;

(*f*) if any of the parties disputes the correctness of the findings of the appropriate laboratory, or disputes the correctness of the methods of analysis or test adopted by the appropriate laboratory, require the opposite party or the complainant to submit in writing his objections with regard to the report made by the appropriate laboratory;

(*g*) give a reasonable opportunity to the complainant as well as the opposite party of being heard as to the correctness or otherwise of the report made by the appropriate laboratory and also as to the objection made in relation thereto under clause (*f*) and issue an appropriate order under section 39.

(*3*) The District Commission shall, if the complaint admitted by it under sub-section (*2*) of section 36 relates to goods in respect of which the procedure specified in sub-section (*2*) cannot be followed, or if the complaint relates to any services,—

(*a*) refer a copy of such complaint to the opposite party directing him to give his version of the case within a period of thirty days or such extended period not exceeding fifteen days as may be granted by the District Commission;

(*b*) if the opposite party, on receipt of a copy of the complaint, referred to him under clause (*a*) denies or disputes the allegations contained in the complaint, or omits or fails to take any action to represent his case within the time given by the District Commission, it shall proceed to settle the consumer dispute—

(*i*) on the basis of evidence brought to its notice by the complainant and the opposite party, if the opposite party denies or disputes the allegations contained in the complaint, or

(*ii*) *ex parte* on the basis of evidence brought to its notice by the complainant, where the opposite party omits or fails to take any action to represent his case within the time given by the Commission;

(*c*) decide the complaint on merits if the complainant fails to appear on the date of hearing.

(*4*) For the purposes of sub-sections (*2*) and (*3*), the District Commission may, by order, require an electronic service provider to provide such information, documents or records, as may be specified in that order.

(*5*) No proceedings complying with the procedure laid down in sub-sections (*1*) and (*2*) shall be called in question in any court on the ground that the principles of natural justice have not been complied with.

(*6*) Every complaint shall be heard by the District Commission on the basis of affidavit and documentary evidence placed on record:

Provided that where an application is made for hearing or for examination of parties in person or through video conferencing, the District Commission may, on sufficient cause being shown, and after recording its reasons in writing, allow the same.

(*7*) Every complaint shall be disposed of as expeditiously as possible and endeavour shall be made to decide the complaint within a period of three months from the date of receipt of notice by opposite party where the complaint does not require analysis or testing of commodities and within five months if it requires analysis or testing of commodities:

Provided that no adjournment shall ordinarily be granted by the District Commission unless sufficient cause is shown and the reasons for grant of adjournment have been recorded in writing by the Commission:

Provided further that the District Commission shall make such orders as to the costs occasioned by the adjournment as may be specified by regulations:

Provided also that in the event of a complaint being disposed of after the period so specified, the District Commission shall record in writing, the reasons for the same at the time of disposing of the said complaint.

(*8*) Where during the pendency of any proceeding before the District Commission, if it appears necessary, it may pass such interim order as is just and proper in the facts and circumstances of the case.

(*9*) For the purposes of this section, the District Commission shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 while trying a suit in respect of the following matters, namely:— 5 of 1908.

(*a*) the summoning and enforcing the attendance of any defendant or witness and examining the witness on oath;

(*b*) requiring the discovery and production of any document or other material object as evidence;

(*c*) receiving of evidence on affidavits;

(*d*) the requisitioning of the report of the concerned analysis or test from the appropriate laboratory or from any other relevant source;

(*e*) issuing of commissions for the examination of any witness, or document; and (*f*) any other matter which may be prescribed by the Central Government.

(*10*) Every proceeding before the District Commission shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228 of the Indian Penal Code, and the District Commission shall be deemed to be a criminal court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

45 of 1860.

2 of 1974.

(*11*) Where the complainant is a consumer referred to in sub-clause (*v*) of clause (*5*) of section 2, the provisions of Order I Rule 8 of the First Schedule to the Code of Civil Procedure, 1908 shall apply subject to the modification that every reference therein to a suit or decree shall be construed as a reference to a complaint or the order of the District Commission thereon.

5 of 1908.

(*12*) In the event of death of a complainant who is a consumer or of the opposite party against whom the complaint has been filed, the provisions of Order XXII of the First Schedule to the Code of Civil Procedure, 1908 shall apply subject to the modification that every reference therein to the plaintiff and the defendant shall be construed as reference to a complainant or the opposite party, as the case may be.

5 of 1908.

Findings of District Commission.

39. (*1*) Where the District Commission is satisfied that the goods complained against suffer from any of the defects specified in the complaint or that any of the allegations contained in the complaint about the services or any unfair trade practices, or claims for compensation under product liability are proved, it shall issue an order to the opposite party directing him to do one or more of the following, namely:—

(*a*) to remove the defect pointed out by the appropriate laboratory from the goods in question;

(*b*) to replace the goods with new goods of similar description which shall be free from any defect;

(*c*) to return to the complainant the price, or, as the case may be, the charges paid by the complainant along with such interest on such price or charges as may be decided;

(*d*) to pay such amount as may be awarded by it as compensation to the consumer for any loss or injury suffered by the consumer due to the negligence of the opposite party:

Provided that the District Commission shall have the power to grant punitive damages in such circumstances as it deems fit;

(*e*) to pay such amount as may be awarded by it as compensation in a product liability action under Chapter VI;

(*f*) to remove the defects in goods or deficiencies in the services in question;

(*g*) to discontinue the unfair trade practice or restrictive trade practice and not to repeat them;

(*h*) not to offer the hazardous or unsafe goods for sale;

(*i*) to withdraw the hazardous goods from being offered for sale;

(*j*) to cease manufacture of hazardous goods and to desist from offering services which are hazardous in nature;

(*k*) to pay such sum as may be determined by it, if it is of the opinion that loss or injury has been suffered by a large number of consumers who are not identifiable conveniently:

Provided that the minimum amount of sum so payable shall not be less than twenty-five per cent. of the value of such defective goods sold or service provided, as the case may be, to such consumers;

(*l*) to issue corrective advertisement to neutralise the effect of misleading advertisement at the cost of the opposite party responsible for issuing such misleading advertisement;

(*m*) to provide for adequate costs to parties; and

(*n*) to cease and desist from issuing any misleading advertisement.

(*2*) Any amount obtained under sub-section (*1*) shall be credited to such fund and utilised in such manner as may be prescribed.

(*3*) In any proceeding conducted by the President and a member and if they differ on any point or points, they shall state the point or points on which they differ and refer the same to another member for hearing on such point or points and the opinion of the majority shall be the order of the District Commission:

Provided that the other member shall give his opinion on such point or points referred to him within a period of one month from the date of such reference.

(*4*) Every order made by the District Commission under sub-section (*1*) shall be signed by the President and the member who conducted the proceeding:

Provided that where the order is made as per majority opinion under sub-section (*3*), such order shall also be signed by the other member.

Review by District Commission in certain cases.

40. The District Commission shall have the power to review any of the order passed by it if there is an error apparent on the face of the record, either of its own motion or on an application made by any of the parties within thirty days of such order.

Appeal against order of District Commission.

41. Any person aggrieved by an order made by the District Commission may prefer an appeal against such order to the State Commission on the grounds of facts or law within a period of forty-five days from the date of the order, in such form and manner, as may be prescribed:

Provided that the State Commission may entertain an appeal after the expiry of the said period of forty-five days, if it is satisfied that there was sufficient cause for not filing it within that period:

Provided further that no appeal by a person, who is required to pay any amount in terms of an order of the District Commission, shall be entertained by the State Commission unless the appellant has deposited fifty per cent. of that amount in the manner as may be prescribed:

Provided also that no appeal shall lie from any order passed under sub-section (*1*) of section 81 by the District Commission pursuant to a settlement by mediation under section 80.

Establishment of State Consumer Disputes Redressal Commission.

42. (*1*) The State Government shall, by notification, establish a State Consumer Disputes Redressal Commission, to be known as the State Commission, in the State.

(*2*) The State Commission shall ordinarily function at the State capital and perform its functions at such other places as the State Government may in consultation with the State Commission notify in the Official Gazette:

Provided that the State Government may, by notification, establish regional benches of the State Commission, at such places, as it deems fit.

(*3*) Each State Commission shall consist of—

(*a*) a President; and

(*b*) not less than four or not more than such number of members as may be prescribed in consultation with the Central Government.

43. The Central Government may, by notification, make rules to provide for the qualification for appointment, method of recruitment, procedure of appointment, term of office, resignation and removal of the President and members of the State Commission.

Qualifications, etc., of President and members of State Commission.

44. The State Government may, by notification, make rules to provide for salaries and allowances and other terms and conditions of service of the President and members of the State Commission.

Salaries, allowances and other terms and conditions of service of President and members of State Commission.

45. Any person appointed as President or, as the case may be, a member of the State Commission immediately before the commencement of this Act shall hold office as such, as President or member, as the case may be, till the completion of his term.

Transitional provision.

46. (*1*) The State Government shall determine the nature and categories of the officers and other employees required to assist the State Commission in the discharge of its functions and provide the Commission with such officers and other employees as it may think fit.

Officers and employees of State Commission.

(*2*) The officers and other employees of the State Commission shall discharge their functions under the general superintendence of the President.

(*3*) The salaries and allowances payable to and the other terms and conditions of service of, the officers and other employees of the State Commission shall be such as may be prescribed.

47. (*1*) Subject to the other provisions of this Act, the State Commission shall have jurisdiction—

Jurisdiction of State Commission.

(*a*) to entertain—

(*i*) complaints where the value of the goods or services paid as consideration, exceeds rupees one crore, but does not exceed rupees ten crore:

Provided that where the Central Government deems it necessary so to do, it may prescribe such other value, as it deems fit;

(*ii*) complaints against unfair contracts, where the value of goods or services paid as consideration does not exceed ten crore rupees;

(*iii*) appeals against the orders of any District Commission within the State; and

(*b*) to call for the records and pass appropriate orders in any consumer dispute which is pending before or has been decided by any District Commission within the State, where it appears to the State Commission that such District Commission has exercised a jurisdiction not vested in it by law, or has failed to exercise a jurisdiction so vested or has acted in exercise of its jurisdiction illegally or with material irregularity.

(*2*) The jurisdiction, powers and authority of the State Commission may be exercised by Benches thereof, and a Bench may be constituted by the President with one or more members as the President may deem fit:

Provided that the senior-most member shall preside over the Bench.

(*3*) Where the members of a Bench differ in opinion on any point, the points shall be decided according to the opinion of the majority, if there is a majority, but if the members are equally divided, they shall state the point or points on which they differ, and make a reference to the President who shall either hear the point or points himself or refer the case for hearing on such point or points by one or more of the other members and such point or points shall be decided according to the opinion of the majority of the members who have heard the case, including those who first heard it:

Provided that the President or the other members, as the case may be, shall give opinion on the point or points so referred within a period of one month from the date of such reference.

(*4*) A complaint shall be instituted in a State Commission within the limits of whose jurisdiction,—

(*a*) the opposite party or each of the opposite parties, where there are more than one, at the time of the institution of the complaint, ordinarily resides or carries on business or has a branch office or personally works for gain; or

(*b*) any of the opposite parties, where there are more than one, at the time of the institution of the complaint, actually and voluntarily resides, or carries on business or has a branch office or personally works for gain, provided in such case, the permission of the State Commission is given; or

(*c*) the cause of action, wholly or in part, arises; or

(*d*) the complainant resides or personally works for gain.

Transfer of cases.

48. On the application of the complainant or of its own motion, the State Commission may, at any stage of the proceeding, transfer any complaint pending before a District Commission to another District Commission within the State if the interest of justice so requires.

Procedure applicable to State Commission.

49. (*1*) The provisions relating to complaints under sections 35, 36, 37, 38 and 39 shall, with such modifications as may be necessary, be applicable to the disposal of complaints by the State Commission.

(*2*) Without prejudice to the provisions of sub-section (*1*), the State Commission may also declare any terms of contract, which is unfair to any consumer, to be null and void.

Review by State Commission in certain cases.

50. The State Commission shall have the power to review any of the order passed by it if there is an error apparent on the face of the record, either of its own motion or on an application made by any of the parties within thirty days of such order.

Appeal to National Commission.

51. (*1*) Any person aggrieved by an order made by the State Commission in exercise of its powers conferred by sub-clause (*i*) or (*ii*) of clause (*a*) of sub-section (*1*) of section 47 may prefer an appeal against such order to the National Commission within a period of thirty days from the date of the order in such form and manner as may be prescribed:

Provided that the National Commission shall not entertain the appeal after the expiry of the said period of thirty days unless it is satisfied that there was sufficient cause for not filing it within that period:

Provided further that no appeal by a person, who is required to pay any amount in terms of an order of the State Commission, shall be entertained by the National Commission unless the appellant has deposited fifty per cent. of that amount in the manner as may be prescribed.

(*2*) Save as otherwise expressly provided under this Act or by any other law for the time being in force, an appeal shall lie to the National Commission from any order passed in appeal by any State Commission, if the National Commission is satisfied that the case involves a substantial question of law.

(*3*) In an appeal involving a question of law, the memorandum of appeal shall precisely state the substantial question of law involved in the appeal.

(*4*) Where the National Commission is satisfied that a substantial question of law is involved in any case, it shall formulate that question and hear the appeal on that question:

Provided that nothing in this sub-section shall be deemed to take away or abridge the power of the National Commission to hear, for reasons to be recorded in writing, the appeal on any other substantial question of law, if it is satisfied that the case involves such question of law.

(*5*) An appeal may lie to the National Commission under this section from an order passed *ex parte* by the State Commission.

Hearing of appeal.

52. An appeal filed before the State Commission or the National Commission, as the case may be, shall be heard as expeditiously as possible and every endeavour shall be made to dispose of the appeal within a period of ninety days from the date of its admission:

Provided that no adjournment shall ordinarily be granted by the State Commission or the National Commission, as the case may be, unless sufficient cause is shown and the reasons for grant of adjournment have been recorded in writing by such Commission:

Provided further that the State Commission or the National Commission, as the case may be, shall make such orders as to the costs occasioned by the adjournment, as may be specified by regulations:

Provided also that in the event of an appeal being disposed of after the period so specified, the State Commission or the National Commission, as the case may be, shall record in writing the reasons for the same at the time of disposing of the said appeal.

Establishment of National Consumer Disputes Redressal Commission.

53. (*1*) The Central Government shall, by notification, establish a National Consumer Disputes Redressal Commission, to be known as the National Commission.

(*2*) The National Commission shall ordinarily function at the National Capital Region and perform its functions at such other places as the Central Government may in consultation with the National Commission notify in the Official Gazette:

Provided that the Central Government may, by notification, establish regional Benches of the National Commission, at such places, as it deems fit.

Composition of National Commission.

54. The National Commission shall consist of—

(*a*) a President; and

(*b*) not less than four and not more than such number of members as may be prescribed.

Qualifications, etc., of President and members of National Commission.

55. (*1*) The Central Government may, by notification, make rules to provide for qualifications, appointment, term of office, salaries and allowances, resignation, removal and other terms and conditions of service of the President and members of the National Commission:

Provided that the President and members of the National Commission shall hold office for such term as specified in the rules made by the Central Government but not exceeding five years from the date on which he enters upon his office and shall be eligible for re-appointment:

Provided further that no President or members shall hold office as such after he has attained such age as specified in the rules made by the Central Government which shall not exceed,—

(*a*) in the case of the President, the age of seventy years;

(*b*) in the case of any other member, the age of sixty-seven years.

(*2*) Neither the salary and allowances nor the other terms and conditions of service of President and members of the National Commission shall be varied to his disadvantage after his appointment.

Transitional provision.

56. The President and every other member appointed immediately before the commencement of section 177 of the Finance Act, 2017 shall continue to be governed by the provisions of the Consumer Protection Act, 1986 and the rules made thereunder as if this Act had not come into force. 7 of 2017. 68 of 1986.

Other officers and employees of National Commission.

57. (*1*) The Central Government shall provide, in consultation with the President of the National Commission, such number of officers and other employees to assist the National Commission in the discharge of its functions as it may think fit.

(*2*) The officers and other employees of the National Commission shall discharge their functions under the general superintendence of the President of the National Commission.

(*3*) The salaries and allowances payable to, and the other terms and conditions of service of, the officers and other employees of the National Commission shall be such as may be prescribed.

Jurisdiction of National Commission.

58. (*1*) Subject to the other provisions of this Act, the National Commission shall have jurisdiction—

(*a*) to entertain—

(*i*) complaints where the value of the goods or services paid as consideration exceeds rupees ten crore:

Provided that where the Central Government deems it necessary so to do, it may prescribe such other value, as it deems fit;

(*ii*) complaints against unfair contracts, where the value of goods or services paid as consideration exceeds ten crore rupees;

(*iii*) appeals against the orders of any State Commission;

(*iv*) appeals against the orders of the Central Authority; and

(*b*) to call for the records and pass appropriate orders in any consumer dispute which is pending before or has been decided by any State Commission where it appears to the National Commission that such State Commission has exercised a jurisdiction not vested in it by law, or has failed to exercise a jurisdiction so vested, or has acted in the exercise of its jurisdiction illegally or with material irregularity.

(*2*) The jurisdiction, powers and authority of the National Commission may be exercised by Benches thereof and a Bench may be constituted by the President with one or more members as he may deem fit:

Provided that the senior-most member of the Bench shall preside over the Bench.

(*3*) Where the members of a Bench differ in opinion on any point, the points shall be decided according to the opinion of the majority, if there is a majority, but if the members are equally divided, they shall state the point or points on which they differ, and make a reference to the President who shall either hear the point or points himself or refer the case for hearing on such point or points by one or more of the other members and such point or points shall be decided according to the opinion of the majority of the members who have heard the case, including those who first heard it:

Provided that the President or the other member, as the case may be, shall give opinion on the point or points so referred within a period of two months from the date of such reference.

Procedure applicable to National Commission.

59. (*1*) The provisions relating to complaints under sections 35, 36, 37, 38 and 39 shall, with such modifications as may be considered necessary, be applicable to the disposal of complaints by the National Commission.

(*2*) Without prejudice to sub-section (*1*), the National Commission may also declare any terms of contract, which is unfair to any consumer to be null and void.

Review by National Commission in certain cases.

60. The National Commission shall have the power to review any of the order passed by it if there is an error apparent on the face of the record, either of its own motion or on an application made by any of the parties within thirty days of such order.

Power to set aside *ex parte* orders.

61. Where an order is passed by the National Commission *ex parte*, the aggrieved party may make an application to the Commission for setting aside such order.

Transfer of cases.

62. On the application of the complainant or of its own motion, the National Commission may, at any stage of the proceeding, in the interest of justice, transfer any complaint pending before the District Commission of one State to a District Commission of another State or before one State Commission to another State Commission.

Vacancy in office of President of National Commission.

63. When the office of President of the National Commission is vacant or a person occupying such office is, by reason of absence or otherwise, unable to perform the duties of his office, these shall be performed by the senior-most member of the National Commission:

Provided that where a retired Judge of a High Court or a person who has been a Judicial Member is a member of the National Commission, such member or where the number of such members is more than one, the senior-most person amongst such members, shall preside over the National Commission in the absence of President of that Commission.

Vacancies or defects in appointment not to invalidate orders.

64. No act or proceeding of the District Commission, the State Commission or the National Commission shall be invalid by reason only of the existence of any vacancy amongst its members or any defect in the constitution thereof.

Service of notice, etc.

65. (*1*) All notices, required by this Act to be served, shall be served by delivering or transmitting a copy thereof by registered post acknowledgment due addressed to opposite party against whom complaint is made or to the complainant by speed post or by such courier service, approved by the District Commission, the State Commission or the National Commission, as the case may be, or by any other mode of transmission of documents including electronic means.

(*2*) Without prejudice to the provisions contained in sub-section (*1*), the notice required by this Act may be served on an electronic service provider at the address provided by it on the electronic platform from where it provides its services as such and for this purpose, the electronic service provider shall designate a nodal officer to accept and process such notices.

(*3*) When an acknowledgment or any other receipt purporting to be signed by the opposite party or his agent or, as the case may be, by the complainant is received by the District Commission, the State Commission or the National Commission, as the case may be, or postal article containing the notice is received back by such District Commission, State Commission or the National Commission, with an endorsement purporting to have been made by a postal employee or by any person authorised by the courier service to the effect that the opposite party or his agent or complainant had refused to take delivery of the postal article containing the notice or had refused to accept the notice by any other means specified in sub-section (*1*) when tendered or transmitted to him, the District Commission or the State Commission or the National Commission, as the case may be, shall declare that the notice has been duly served on the opposite party or to the complainant, as the case may be:

Provided that where the notice was properly addressed, pre-paid and duly sent by registered post acknowledgment due, a declaration referred to in this sub-section shall be made notwithstanding the fact that the acknowledgment has been lost or misplaced, or for any other reason, has not been received by the District Commission, the State Commission or the National Commission, as the case may be, within thirty days from the date of issue of notice.

(*4*) All notices required to be served on an opposite party or to complainant, as the case may be, shall be deemed to be sufficiently served, if addressed in the case of the opposite party, to the place where business or profession is carried on, and in case of the complainant, the place where such person actually and voluntarily resides.

Experts to assist National Commission or State Commission.

66. Where the National Commission or the State Commission, as the case may be, on an application by a complainant or otherwise, is of the opinion that it involves the larger interest of consumers, it may direct any individual or organisation or expert to assist the National Commission or the State Commission, as the case may be.

Appeal against order of National Commission.

67. Any person, aggrieved by an order made by the National Commission in exercise of its powers conferred by sub-clause (*i*) or (*ii*) of clause (*a*) of sub-section (*1*) of section 58, may prefer an appeal against such order to the Supreme Court within a period of thirty days from the date of the order:

Provided that the Supreme Court may entertain an appeal after the expiry of the said period of thirty days if it is satisfied that there was sufficient cause for not filing it within that period:

Provided further that no appeal by a person who is required to pay any amount in terms of an order of the National Commission shall be entertained by the Supreme Court unless that person has deposited fifty per cent. of that amount in the manner as may be prescribed.

Finality of orders.

68. Every order of a District Commission or the State Commission or the National Commission, as the case may be, shall, if no appeal has been preferred against such order under the provisions of this Act, be final.

Limitation period.

69. (*1*) The District Commission, the State Commission or the National Commission shall not admit a complaint unless it is filed within two years from the date on which the cause of action has arisen.

(*2*) Notwithstanding anything contained in sub-section (*1*), a complaint may be entertained after the period specified in sub-section (*1*), if the complainant satisfies the District Commission, the State Commission or the National Commission, as the case may be, that he had sufficient cause for not filing the complaint within such period:

Provided that no such complaint shall be entertained unless the District Commission or the State Commission or the National Commission, as the case may be, records its reasons for condoning such delay.

Administrative control.

70. (*1*) The National Commission shall have the authority to lay down such adequate standards in consultation with the Central Government from time to time, for better protection of the interests of consumers and for that purpose, shall have administrative control over all the State Commissions in the following matters, namely:—

(*a*) monitoring performance of the State Commissions in terms of their disposal by calling for periodical returns regarding the institution, disposal and pendency of cases;

(*b*) investigating into any allegations against the President and members of a State Commission and submitting inquiry report to the State Government concerned along with copy endorsed to the Central Government for necessary action;

(*c*) issuance of instructions regarding adoption of uniform procedure in the hearing of matters, prior service of copies of documents produced by one party to the opposite parties, furnishing of english translation of judgments written in any language, speedy grant of copies of documents;

(*d*) overseeing the functioning of the State Commission or the District Commission either by way of inspection or by any other means, as the National Commission may like to order from time to time, to ensure that the objects and purposes of the Act are best served and the standards set by the National Commission are implemented without interfering with their quasi-judicial freedom.

(*2*) There shall be a monitoring cell to be constituted by the President of the National Commission to oversee the functioning of the State Commissions from the administrative point of view.

(*3*) The State Commission shall have administrative control over all the District Commissions within its jurisdiction in all matters referred to in sub-section (*1*).

(*4*) The National Commission and the State Commissions shall furnish to the Central Government periodically or as and when required, any information including the pendency of cases in such form and manner as may be prescribed.

(*5*) The State Commission shall furnish, periodically or as and when required to the State Government any information including pendency of cases in such form and manner as may be prescribed.

Enforcement of orders of District Commission, State Commission and National Commission.

71. Every order made by a District Commission, State Commission or the National Commission shall be enforced by it in the same manner as if it were a decree made by a Court in a suit before it and the provisions of Order XXI of the First Schedule to the Code of Civil Procedure, 1908 shall, as far as may be, applicable, subject to the modification that every reference therein to the decree shall be construed as reference to the order made under this Act.

5 of 1908.

Penalty for non-compliance of order.

72. (*1*) Whoever fails to comply with any order made by the District Commission or the State Commission or the National Commission, as the case may be, shall be punishable with imprisonment for a term which shall not be less than one month, but which may extend to three years, or with fine, which shall not be less than twenty-five thousand rupees, but which may extend to one lakh rupees, or with both.

2 of 1974.

(*2*) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the District Commission, the State Commission or the National Commission, as the case may be, shall have the power of a Judicial Magistrate of first class for the trial of offences under sub-section (*1*), and on conferment of such powers, the District Commission or the State Commission or the National Commission, as the case may be, shall be deemed to be a Judicial Magistrate of first class for the purposes of the Code of Criminal Procedure, 1973.

(*3*) Save as otherwise provided, the offences under sub-section (*1*) shall be tried summarily by the District Commission or the State Commission or the National Commission, as the case may be.

2 of 1974.

Appeal against order passed under section 72.

73. (*1*) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, where an order is passed under sub-section (*1*) of section 72, an appeal shall lie, both on facts and on law from—

(*a*) the order made by the District Commission to the State Commission;

(*b*) the order made by the State Commission to the National Commission; and

(*c*) the order made by the National Commission to the Supreme Court.

(*2*) Except as provided in sub-section (*1*), no appeal shall lie before any court, from any order of a District Commission or a State Commission or the National Commission, as the case may be.

(*3*) Every appeal under this section shall be preferred within a period of thirty days from the date of order of a District Commission or a State Commission or the National Commission, as the case may be:

Provided that the State Commission or the National Commission or the Supreme Court, as the case may be, may entertain an appeal after the expiry of the said period of thirty days, if it is satisfied that the appellant had sufficient cause for not preferring the appeal within the said period of thirty days.

CHAPTER V

MEDIATION

Establishment of consumer mediation cell.

74. (*1*) The State Government shall establish, by notification, a consumer mediation cell to be attached to each of the District Commissions and the State Commissions of that State.

(*2*) The Central Government shall establish, by notification, a consumer mediation cell to be attached to the National Commission and each of the regional Benches.

(*3*) A consumer mediation cell shall consist of such persons as may be prescribed.

(*4*) Every consumer mediation cell shall maintain—

(*a*) a list of empanelled mediators;

(*b*) a list of cases handled by the cell;

(*c*) record of proceeding; and

(*d*) any other information as may be specified by regulations.

(*5*) Every consumer mediation cell shall submit a quarterly report to the District Commission, State Commission or the National Commission to which it is attached, in the manner specified by regulations.

Empanelment of mediators.

75. (*1*) For the purpose of mediation, the National Commission or the State Commission or the District Commission, as the case may be, shall prepare a panel of the mediators to be maintained by the consumer mediation cell attached to it, on the recommendation of a selection committee consisting of the President and a member of that Commission.

(*2*) The qualifications and experience required for empanelment as mediator, the procedure for empanelment, the manner of training empanelled mediators, the fee payable to empanelled mediator, the terms and conditions for empanelment, the code of conduct for empanelled mediators, the grounds on which, and the manner in which, empanelled mediators shall be removed or empanelment shall be cancelled and other matters relating thereto, shall be such as may be specified by regulations.

(*3*) The panel of mediators prepared under sub-section (*1*) shall be valid for a period of five years, and the empanelled mediators shall be eligible to be considered for re-empanelment for another term, subject to such conditions as may be specified by regulations.

Nomination of mediators from panel.

76. The District Commission, the State Commission or the National Commission shall, while nominating any person from the panel of mediators referred to in section 75, consider his suitability for resolving the consumer dispute involved.

Duty of mediator to disclose certain facts.

77. It shall be the duty of the mediator to disclose—

(*a*) any personal, professional or financial interest in the outcome of the consumer dispute;

(*b*) the circumstances which may give rise to a justifiable doubt as to his independence or impartiality; and

(*c*) such other facts as may be specified by regulations.

Replacement of mediator in certain cases.

78. Where the District Commission or the State Commission or the National Commission, as the case may be, is satisfied, on the information furnished by the mediator or on the information received from any other person including parties to the complaint and after hearing the mediator, it shall replace such mediator by another mediator.

Procedure for mediation.

79. (*1*) The mediation shall be held in the consumer mediation cell attached to the District Commission, the State Commission or the National Commission, as the case may be.

(*2*) Where a consumer dispute is referred for mediation by the District Commission or the State Commission or the National Commission, as the case may be, the mediator nominated by such Commission shall have regard to the rights and obligations of the parties, the usages of trade, if any, the circumstances giving rise to the consumer dispute and such other relevant factors, as he may deem necessary and shall be guided by the principles of natural justice while carrying out mediation.

(*3*) The mediator so nominated shall conduct mediation within such time and in such manner as may be specified by regulations.

Settlement through mediation.

80. (*1*) Pursuant to mediation, if an agreement is reached between the parties with respect to all of the issues involved in the consumer dispute or with respect to only some of the issues, the terms of such agreement shall be reduced to writing accordingly, and signed by the parties to such dispute or their authorised representatives.

(*2*) The mediator shall prepare a settlement report of the settlement and forward the signed agreement along with such report to the concerned Commission.

(*3*) Where no agreement is reached between the parties within the specified time or the mediator is of the opinion that settlement is not possible, he shall prepare his report accordingly and submit the same to the concerned Commission.

Recording settlement and passing of order.

81. (*1*) The District Commission or the State Commission or the National Commission, as the case may be, shall, within seven days of the receipt of the settlement report, pass suitable order recording such settlement of consumer dispute and dispose of the matter accordingly.

(*2*) Where the consumer dispute is settled only in part, the District Commission or the State Commission or the National Commission, as the case may be, shall record settlement of the issues which have been so settled and continue to hear other issues involved in such consumer dispute.

(*3*) Where the consumer dispute could not be settled by mediation, the District Commission or the State Commission or the National Commission, as the case may be, shall continue to hear all the issues involved in such consumer dispute.

CHAPTER VI

PRODUCT LIABILITY

Application of Chapter.

82. This Chapter shall apply to every claim for compensation under a product liability action by a complainant for any harm caused by a defective product manufactured by a product manufacturer or serviced by a product service provider or sold by a product seller.

Product liability action.

83. A product liability action may be brought by a complainant against a product manufacturer or a product service provider or a product seller, as the case may be, for any harm caused to him on account of a defective product.

Liability of product manufacturer.

84. (*1*) A product manufacturer shall be liable in a product liability action, if—

(*a*) the product contains a manufacturing defect; or

(*b*) the product is defective in design; or

(*c*) there is a deviation from manufacturing specifications; or

(*d*) the product does not conform to the express warranty; or

(*e*) the product fails to contain adequate instructions of correct usage to prevent any harm or any warning regarding improper or incorrect usage.

(*2*) A product manufacturer shall be liable in a product liability action even if he proves that he was not negligent or fraudulent in making the express warranty of a product.

Liability of product service provider.

85. A product service provider shall be liable in a product liability action, if—

(*a*) the service provided by him was faulty or imperfect or deficient or inadequate in quality, nature or manner of performance which is required to be provided by or under any law for the time being in force, or pursuant to any contract or otherwise; or

(*b*) there was an act of omission or commission or negligence or conscious withholding any information which caused harm; or

(*c*) the service provider did not issue adequate instructions or warnings to prevent any harm; or

(*d*) the service did not conform to express warranty or the terms and conditions of the contract.

Liability of product sellers.

86. A product seller who is not a product manufacturer shall be liable in a product liability action, if—

(*a*) he has exercised substantial control over the designing, testing, manufacturing, packaging or labelling of a product that caused harm; or

(*b*) he has altered or modified the product and such alteration or modification was the substantial factor in causing the harm; or

(*c*) he has made an express warranty of a product independent of any express warranty made by a manufacturer and such product failed to conform to the express warranty made by the product seller which caused the harm; or

(*d*) the product has been sold by him and the identity of product manufacturer of such product is not known, or if known, the service of notice or process or warrant cannot be effected on him or he is not subject to the law which is in force in India or the order, if any, passed or to be passed cannot be enforced against him; or

(*e*) he failed to exercise reasonable care in assembling, inspecting or maintaining such product or he did not pass on the warnings or instructions of the product manufacturer regarding the dangers involved or proper usage of the product while selling such product and such failure was the proximate cause of the harm.

Exceptions to product liability action.

87. (*1*) A product liability action cannot be brought against the product seller if, at the time of harm, the product was misused, altered, or modified.

(*2*) In any product liability action based on the failure to provide adequate warnings or instructions, the product manufacturer shall not be liable, if—

(*a*) the product was purchased by an employer for use at the workplace and the product manufacturer had provided warnings or instructions to such employer;

(*b*) the product was sold as a component or material to be used in another product and necessary warnings or instructions were given by the product manufacturer to the purchaser of such component or material, but the harm was caused to the complainant by use of the end product in which such component or material was used;

(*c*) the product was one which was legally meant to be used or dispensed only by or under the supervision of an expert or a class of experts and the product manufacturer had employed reasonable means to give the warnings or instructions for usage of such product to such expert or class of experts; or

(*d*) the complainant, while using such product, was under the influence of alcohol or any prescription drug which had not been prescribed by a medical practitioner.

(*3*) A product manufacturer shall not be liable for failure to instruct or warn about a danger which is obvious or commonly known to the user or consumer of such product or which, such user or consumer, ought to have known, taking into account the characteristics of such product.

CHAPTER VII

OFFENCES AND PENALTIES

Penalty for non-compliance of direction of Central Authority.

88. Whoever, fails to comply with any direction of the Central Authority under sections 20 and 21, shall be punished with imprisonment for a term which may extend to six months or with fine which may extend to twenty lakh rupees, or with both.

Punishment for false or misleading advertisement.

89. Any manufacturer or service provider who causes a false or misleading advertisement to be made which is prejudicial to the interest of consumers shall be punished with imprisonment for a term which may extend to two years and with fine which may extend to ten lakh rupees; and for every subsequent offence, be punished with imprisonment for a term which may extend to five years and with fine which may extend to fifty lakh rupees.

Punishment for manufacturing for sale or storing, selling or distributing or importing products containing adulterant.

90. (*1*) Whoever, by himself or by any other person on his behalf, manufactures for sale or stores or sells or distributes or imports any product containing an adulterant shall be punished, if such act—

(*a*) does not result in any injury to the consumer, with imprisonment for a term which may extend to six months and with fine which may extend to one lakh rupees;

(*b*) causing injury not amounting to grievous hurt to the consumer, with imprisonment for a term which may extend to one year and with fine which may extend to three lakh rupees;

(*c*) causing injury resulting in grievous hurt to the consumer, with imprisonment for a term which may extend to seven years and with fine which may extend to five lakh rupees; and

(*d*) results in the death of a consumer, with imprisonment for a term which shall not be less than seven years, but which may extend to imprisonment for life and with fine which shall not be less than ten lakh rupees.

(*2*) The offences under clauses (*c*) and (*d*) of sub-section (*1*) shall be cognizable and non-bailable.

(*3*) Notwithstanding the punishment under sub-section (*1*), the court may, in case of first conviction, suspend any licence issued to the person referred to in that sub-section, under any law for the time being in force, for a period up to two years, and in case of second or subsequent conviction, cancel the licence.

Explanation.—For the purposes of this section,—

(*a*) "adulterant" means any material including extraneous matter which is employed or used for making a product unsafe;

(*b*) "grievous hurt" shall have the same meaning as assigned to it in section 320 of the Indian Penal Code.

45 of 1860.

Punishment for manufacturing for sale or for storing or selling or distributing or importing spurious goods.

91. (*1*) Whoever, by himself or by any other person on his behalf, manufactures for sale or stores or sells or distributes or imports any spurious goods shall be punished, if such act—

(*a*) causing injury not amounting to grievous hurt to the consumer, with imprisonment for a term which may extend to one year and with fine which may extend to three lakh rupees;

(*b*) causing injury resulting in grievous hurt to the consumer, with imprisonment for a term which may extend to seven years and with fine which may extend to five lakh rupees;

(*c*) results in the death of a consumer, with imprisonment for a term which shall not be less than seven years, but may extend to imprisonment for life and with fine which shall not be less than ten lakh rupees.

(*2*) The offences under clauses (*b*) and (*c*) of sub-section (*1*) shall be cognizable and non-bailable.

(*3*) Notwithstanding the punishment under sub-section (*1*), the court may, in case of first conviction, suspend any licence issued to the person referred to in that sub-section, under any law for the time being in force, for a period up to two years, and in case of second or subsequent conviction, cancel the licence.

Cognizance of offence by court.

92. No cognizance shall be taken by a competent court of any offence under sections 88 and 89 except on a complaint filed by the Central Authority or any officer authorised by it in this behalf.

Vexatious search.

93. The Director General or any other officer, exercising powers under section 22, who knows that there are no reasonable grounds for so doing, and yet—

(*a*) searches, or causes to be searched any premises; or

(*b*) seizes any record, register or other document or article,

shall, for every such offence, be punished with imprisonment for a term which may extend to one year, or with fine which may extend to ten thousand rupees or with both.

CHAPTER VIII

MISCELLANEOUS

Measures to prevent unfair trade practices in e-commerce, direct selling, etc.

94. For the purposes of preventing unfair trade practices in e-commerce, direct selling and also to protect the interest and rights of consumers, the Central Government may take such measures in the manner as may be prescribed.

Presidents, members, Chief Commissioner, Commissioner and certain officers to be public servants.

95. The Presidents and members of the District Commission, the State Commission and the National Commission, and officers and other employees thereof, the Chief Commissioner and the Commissioner of the Central Authority, the Director General, the Additional Director General, the Director, the Joint Director, the Deputy Director and the Assistant Director and all other officers and employees of the Central Authority and other persons performing any duty under this Act, while acting or purporting to act in pursuance of any of the provisions of this Act, shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code. 45 of 1860.

Compounding of offences.

96. (*1*) Any offence punishable under sections 88 and 89, may, either before or after the institution of the prosecution, be compounded, on payment of such amount as may be prescribed:

Provided that no compounding of such offence shall be made without the leave of the court before which a complaint has been filed under section 92:

Provided further that such sum shall not, in any case, exceed the maximum amount of the fine, which may be imposed under this Act for the offence so compounded.

(*2*) The Central Authority or any officer as may be specially authorised by him in this behalf, may compound offences under sub-section (*1*).

(*3*) Nothing in sub-section (*1*) shall apply to person who commits the same or similar offence, within a period of three years from the date on which the first offence, committed by him, was compounded.

Explanation.—For the purposes of this sub-section, any second or subsequent offence committed after the expiry of a period of three years from the date on which the offence was previously compounded, shall be deemed to be a first offence.

(*4*) Where an offence has been compounded under sub-section (*1*), no proceeding or further proceeding, as the case may be, shall be taken against the offender in respect of the offence so compounded.

(*5*) The acceptance of the sum of money for compounding an offence in accordance with sub-section (*1*) by the Central Authority or an officer of the Central Authority empowered in this behalf shall be deemed to amount to an acquittal within the meaning of the Code of Criminal Procedure, 1973. (2 of 1974.)

Manner of crediting penalty.

97. The penalty collected under section 21 and the amount collected under section 96 shall be credited to such fund as may be prescribed.

Protection of action taken in good faith.

98. No suit, prosecution or other legal proceeding shall lie against the Presidents and members of the District Commission, the State Commission and the National Commission, the Chief Commissioner, the Commissioner, any officer or employee and other person performing any duty under this Act, for any act which is in good faith done or intended to be done in pursuance of this Act or under any rule or order made thereunder.

Power to give directions by Central Government.

99. (*1*) Without prejudice to the foregoing provisions of this Act, the Central Authority, shall, in exercise of its powers or the performance of its functions under this Act, be bound by such directions on questions of policy, as the Central Government may give in writing to it from time to time:

Provided that the Central Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section.

(*2*) The decision of the Central Government whether a question is one of policy or not shall be final.

Act not in derogation of any other law.

100. The provisions of this Act shall be in addition to and not in derogation of the provisions of any other law for the time being in force.

Power of Central Government to make rules.

101. (*1*) The Central Government may, by notification, make rules for carrying out any of the provisions contained in this Act.

(*2*) Without prejudice to the generality of the foregoing power, such rules may provide for,—

(*a*) the other class or classes of persons including public utility entities under clause (*19*) of section 2;

(*b*) the contest, lottery, game of chance or skill which are to be exempted under item (*b*) of sub-clause (*iii*) of clause (*47*) of section 2;

(*c*) the manner of issuing bill or cash memo or receipt for goods sold or services rendered under sub-clause (*vii*) of clause (*47*) of section 2;

(*d*) the number of other official or non-official members of the Central Council under clause (*b*) of sub-section (*2*) of section 3;

(*e*) the time and place of meeting of Central Council and the procedure for the transaction of its business under sub-section (*2*) of section 4;

(*f*) the number of Commissioners in the Central Authority under sub-section (*2*) of section 10;

(*g*) the qualifications for appointment, method of recruitment, procedure of appointment, term of office, salaries and allowances, resignation, removal and other terms and conditions of service of the Chief Commissioner and other Commissioners of the Central Authority under section 11;

(*h*) the salaries and allowances payable to, and the other terms and conditions of service of, the officers and other employees of the Central Authority under sub-section (*2*) of section 13;

(*i*) the qualifications for appointment of Director General, Additional Director General, Director, Joint Director, Deputy Director and Assistant Director and the manner of appointment under sub-section (*2*) of section 15;

(*j*) the manner of taking copies or extracts of document, record or article seized or produced before returning to the person under sub-section (*3*) of section 22;

(*k*) the officer and the manner of disposing of articles which are subject to speedy or natural decay under sub-section (*4*) of section 22;

(*l*) the form and manner for preparing annual statement of accounts by the Central Authority in consultation with the Comptroller and Auditor-General of India under sub-section (*1*) of section 26;

(*m*) the form in which, and the time within which, an annual report, other reports and returns may be prepared by the Central Authority under sub-section (*1*) of section 27;

(*n*) the qualifications for appointment, method of recruitment, procedure for appointment, term of office, resignation and removal of President and members of the District Commission under section 29;

(*o*) the other value of goods and services in respect of which the District Commission shall have jurisdiction to entertain complaints under proviso to sub-section (*1*) of section 34;

(*p*) the manner of electronically filing complaint under the proviso to sub-section (*1*) of section 35;

(*q*) the fee, electronic form and the manner of payment of fee for filing complaint under sub-section (*2*) of section 35;

(*r*) the cases which may not be referred for settlement by mediation under sub-section (*1*) of section 37;

(*s*) the manner of authentication of goods sampled in case of the National Commission under clause (*c*) of sub-section (*2*) of section 38;

(*t*) any other matter which may be prescribed under clause (*f*) of sub-section (*9*) of section 38;

(*u*) the fund where the amount obtained may be credited and the manner of utilisation of such amount under sub-section (*2*) of section 39;

(*v*) the form and the manner in which appeal may be preferred to the State Commission under section 41;

(*w*) the qualifications for appointment, method of recruitment, procedure for appointment, term of office, resignation and removal of the President and members of the State Commission under section 43;

(*x*) the other value of goods and services in respect of which the State Commission shall have jurisdiction under the proviso to sub-clause (*i*) of clause (*a*) of sub-section (*1*) of section 47;

(*y*) the form and manner of filing appeal to the National Commission, and the manner of depositing fifty per cent. of the amount before filing appeal, under sub-section (*1*) of section 51;

(*z*) the number of members of the National Commission under clause (*b*) of section 54;

(*za*) the qualifications, appointment, term of office, salaries and allowances, resignation, removal and other terms and conditions of service of the President and members of the National Commission under sub-section (*1*) of section 55;

(*zb*) the salaries and allowances payable to, and other terms and conditions of service of, the officers and other employees of the National Commission under sub-section (*3*) of section 57;

(*zc*) the other value of goods and services in respect of which the National Commission shall have jurisdiction under the proviso to sub-clause (*i*) of clause (*a*) of sub-section (*1*) of section 58;

(*zd*) the manner of depositing fifty per cent. of the amount under the second proviso to section 67;

(*ze*) the form in which the National Commission and the State Commission shall furnish information to the Central Government under sub-section (*4*) of section 70;

(*zf*) the persons in the consumer mediation cell under sub-section (*3*) of section 74;

(*zg*) the measures to be taken by the Central Government to prevent unfair trade practices in e-commerce, direct selling under section 94;

(*zh*) the amount for compounding offences under sub-section (*1*) of section 96;

(*zi*) the fund to which the penalty and amount collected shall be credited under section 97; and

(*zj)* any other matter which is to be, or may be, prescribed, or in respect of which provisions are to be, or may be, made by rules.

Power of State Government to make rules.

102. (*1*) The State Governments may, by notification, make rules for carrying out the provisions of this Act:

Provided that the Central Government may, frame model rules in respect of all or any of the matters with respect to which the State Government may make rules under this section, and where any such model rules have been framed in respect of any such matter, they shall apply to the State until the rules in respect of that matter is made by the State Government and while making any such rules, so far as is practicable, they shall conform to such model rules.

(*2*) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(*a*) the other class or classes of persons including public utility entities under clause (*19*) of section 2;

(*b*) the contest, lottery, game of chance or skill which are to be exempted under item (*b*) of sub-clause (*iii*) of clause (*47*) of section 2;

(*c*) the number of other official or non-official members of the State Council under clause (*b*) of sub-section (*2*) of section 6;

(*d*) the time and place of meeting of the State Council and the procedure for the transaction of its business under sub-section (*4*) of section 6;

(*e*) the number of other official and non-official members of District Council under clause (*b*) of sub-section (*2*) of section 8;

(*f*) the time and place of meeting of the District Council and procedure for the transaction of its business under sub-section (*4*) of section 8;

(*g*) the number of members of the District Commission under clause (*b*) of sub-section (*2*) of section 28;

(*h*) the salaries and allowances payable to, and other terms and conditions of service of, the President and members of the District Commission under section 30;

(*i*) the salaries and allowances payable to, and other terms and conditions of service of, the officers and other employees of the District Commission under sub-section (*3*) of section 33;

(*j*) the manner of authentication of goods sampled by the State Commission and the District Commission under clause (*c*) of sub-section (*2*) of section 38;

(*k*) the manner of depositing fifty per cent. of the amount before filing appeal under second proviso to section 41;

(*l*) the number of members of the State Commission under sub-section (*3*) of section 42;

(*m*) the salaries and allowances payable to, and other terms and conditions of service of, the President and members of the State Commission under section 44;

(*n*) the salaries and allowances payable to, and other terms and conditions of service of, the officers and other employees of the State Commission under sub-section (*3*) of section 46;

(*o*) the form in which the State Commission shall furnish information to the State Government under sub-section (*5*) of section 70;

(*p*) the persons in the consumer mediation cell under sub-section (*3*) of section 74;

(*q*) any other matter which is to be, or may be prescribed, or in respect of which provisions are to be, or may be, made by rules.

Power of National Commission to make regulations.

103. (*1*) The National Commission may, with the previous approval of the Central Government, by notification, make regulations not inconsistent with this Act to provide for all matters for which provision is necessary or expedient for the purpose of giving effect to the provisions of this Act.

(*2*) In particular, and without prejudice to the generality of the foregoing power, such regulations may make provisions for—

(*a*) the costs for adjournment to be imposed by the District Commission under the second proviso to sub-section (*7*) of section 38;

(*b*) the costs for adjournment to be imposed by the State Commission or the National Commission, as the case may be, under the second proviso to section 52;

(*c*) the maintenance of any other information by the consumer mediation cell under sub-section (*4*) of section 74;

(*d*) the manner of submission of quarterly report by consumer mediation cell to the District Commission, the State Commission or the National Commission under sub-section (*5*) of section 74;

(*e*) the qualifications and experience required for empanelment as mediator, the procedure for empanelment, the manner of training empanelled mediators, the fee payable to empanelled mediator, the terms and conditions for empanelment, the code of conduct for empanelled mediators, the grounds on which, and the manner in which, empanelled mediators shall be removed or empanelment shall be cancelled and the other matters relating thereto under sub-section (*2*) of section 75;

(*f*) the conditions for re-empanelment of mediators for another term under sub-section (*3*) of section 75;

(*g*) the other facts to be disclosed by mediators under clause (*c*) of section 77;

(*h*) the time within which, and the manner in which, mediation may be conducted under sub-section (*3*) of section 79; and

(*i*) such other matter for which provision is to be, or may be, made by regulation.

Power of Central Authority to make regulations.

104. (*1*) The Central Authority may, with the previous approval of the Central Government, by notification, make regulations not inconsistent with this Act, for the purpose of giving effect to the provisions of this Act.

(*2*) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:—

(*a*) the procedure for engaging experts and professionals and the number of such experts and professionals under sub-section (*3*) of section 13;

(*b*) the procedure for transaction of business and the allocation of business of the Chief Commissioner and Commissioner under sub-section (*1*) of section 14;

(*c*) the form, manner and time within which, inquiries or investigation made by the Director-General shall be submitted to the Central Authority under sub-section (*5*) of section 15; and

(*d*) such other matter for which provision is to be, or may be, made by regulation.

Rules and regulations to be laid before each House of Parliament.

105. (*1*) Every rule and every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or both Houses agree that the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

(*2*) Every rule made by a State Government under this Act shall be laid as soon as may be after it is made, before the State Legislature.

Power to remove difficulties.

106. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no such order shall be made after the expiry of a period of two years from the commencement of this Act.

Repeal and savings.

68 of 1986. **107.** (*1*) The Consumer Protection Act, 1986 is hereby repealed.

(*2*) Notwithstanding such repeal, anything done or any action taken or purported to have been done or taken under the Act hereby repealed shall, in so far as it is not inconsistent with the provisions of this Act, be deemed to have been done or taken under the corresponding provisions of this Act.

(*3*) The mention of particular matters in sub-section (*2*) shall not be held to prejudice or affect the general application of section 6 of the General Clauses Act, 1897 with regard to the effect of repeal. 10 of 1897.

DR. G. NARAYANA RAJU,
Secretary to the Govt. of India.

UPLOADED BY THE MANAGER, GOVERNMENT OF INDIA PRESS, MINTO ROAD, NEW DELHI–110002
AND PUBLISHED BY THE CONTROLLER OF PUBLICATIONS, DELHI–110054.

MGIPMRND—2606GI(S3)—09-08-2019.

रजिस्ट्री सं. डी.एल.- 33004/99 REGD. No. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-23072020-220661
CG-DL-E-23072020-220661

भाग II—खण्ड 3—उप-खण्ड (i)
PART II—Section 3—Sub-section (i)

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 358] नई दिल्ली, बृहस्पतिवार, जुलाई 23, 2020/श्रावण 1, 1942
No. 358] NEW DELHI, THURSDAY, JULY 23, 2020/SHRAVANA 1, 1942

MINISTRY OF CONSUMER AFFAIRS, FOOD AND PUBLIC DISTRIBUTION

(Department of Consumer Affairs)

NOTIFICATION

New Delhi, 23rd July, 2020

G.S.R. 462(E).—In exercise of the powers conferred by sub-clause (zg) of sub-section (1) of section 101 of the Consumer Protection Act, 2019 (35 of 2019), the Central Government hereby makes the following rules, namely: -

1. **Short title and commencement. —** (1) These rules may be called the Consumer Protection (E-Commerce) Rules, 2020.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Scope and Applicability. –** (1) Save as otherwise expressly provided by the Central Government by notification, these rules shall apply to:

(a) all goods and services bought or sold over digital or electronic network including digital products;

(b) all models of e-commerce, including marketplace and inventory models of e-commerce;

(c) all e-commerce retail, including multi-channel single brand retailers and single brand retailers in single or multiple formats; and

(d) all forms of unfair trade practices across all models of e-commerce:

Provided that these rules shall not apply to any activity of a natural person carried out in a personal capacity not being part of any professional or commercial activity undertaken on a regular or systematic basis.

(2) Notwithstanding anything contained in sub-rule (1), these rules shall apply to a e-commerce entity which is not established in India, but systematically offers goods or services to consumers in India.

3. **Definitions. — (**1) In these rules unless the context otherwise requires, **—**

(a) "Act" means the Consumer Protection Act, 2019 (35 of 2019);

(b) "e-commerce entity" means any person who owns, operates or manages digital or electronic facility or platform for electronic commerce, but does not include a seller offering his goods or services for sale on a marketplace e-commerce entity;

(c) "grievance" includes any complaints to an e-commerce entity regarding violations of the provisions of the Act and the rules made thereunder;

(d) "GSTIN" means the Goods and Services Tax Identification Number as under the Central Goods and Services Tax Act, 2017 (12 of 2017);

(e) "information" shall have the same meaning as to it clause (v) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000);

(f) "inventory e-commerce entity**"** means an e-commerce entity which owns the inventory of goods or services and sells such goods or services directly to the consumers and shall include single brand retailers and multi-channel single brand retailers;

(g) "marketplace e-commerce entity" means an e-commerce entity which provides an information technology platform on a digital or electronic network to facilitate transactions between buyers and sellers;

(h) **"**PAN" means Permanent Account Number as under section 139A of the Income Tax Act, 1961 (43 of 1961);

(i) "platform" means an online interface in the form of any software including a website or a part thereof and applications including mobile applications;

(j) "ranking" means the relative prominence or relevance given to the goods or services offered through a marketplace e-commerce entity as presented, organised or communicated by such entity, irrespective of the technological means used for such presentation, organisation or communication;

(k) **"**seller" means the product seller as defined in clause (37) of section 2 of the Act and shall include any service provider;

(l) "user" means any person who accesses or avails any computer resource of an e-commerce entity.

(2) The words and expressions used herein and not defined, but defined in the Act or in the Information Technology Act, 2000 (21 of 2000) or the rules made thereunder shall have the same meaning as respectively assigned to them in those Acts or rules.

4. **Duties of e-commerce entities. ---**

(1) An e-commerce entity shall:

(a) be a company incorporated under the Companies Act, 1956 (1 of 1956) or the Companies Act, 2013 (18 of 2013) or a foreign company covered under clause (42) of section 2 of the Companies Act, 2013 (18 of 2013) or an office, branch or agency outside India owned or controlled by a person resident in India as provided in sub-clause (iii) of clause (v) of section 2 of the Foreign Exchange Management Act, 1999 (42 of 1999); and

(a) appoint a nodal person of contact or an alternate senior designated functionary who is resident in India, to ensure compliance with the provisions of the Act or the rules made thereunder.

(2) Every e-commerce entity shall provide the following information in a clear and accessible manner on its platform, displayed prominently to its users, namely:--

(क) legal name of the e-commerce entity;

(ख) principal geographic address of its headquarters and all branches;

(ग) name and details of its website; and

(घ) contact details like e-mail address, fax, landline and mobile numbers of customer care as well as of grievance officer.

(3) No e-commerce entity shall adopt any unfair trade practice, whether in the course of business on its platform or otherwise.

(4) Every e-commerce entity shall establish an adequate grievance redressal mechanism having regard to the number of grievances ordinarily received by such entity from India, and shall appoint a grievance officer for consumer grievance redressal, and shall display the name, contact details, and designation of such officer on its platform.

(5) Every e-commerce entity shall ensure that the grievance officer referred to in sub-rule (4) acknowledges the receipt of any consumer complaint within forty-eight hours and redresses the complaint within one month from the date of receipt of the complaint.

(6) Where an e-commerce entity offers imported goods or services for sale, it shall mention the name and details of any importer from whom it has purchased such goods or services, or who may be a seller on its platform.

(7) Every e-commerce entity shall endeavour on a best effort basis to become a partner in the convergence process of the National Consumer Helpline of the Central Government.

(8) No e-commerce entity shall impose cancellation charges on consumers cancelling after confirming purchase unless similar charges are also borne by the e- commerce entity, if they cancel the purchase order unilaterally for any reason.

(9) Every e-commerce entity shall only record the consent of a consumer for the purchase of any good or service offered on its platform where such consent is expressed through an explicit and affirmative action, and no such entity shall record such consent automatically, including in the form of pre-ticked checkboxes.

(10) Every e-commerce entity shall effect all payments towards accepted refund requests of the consumers as prescribed by the Reserve Bank of India or any other competent authority under any law for the time being in force, within a reasonable period of time, or as prescribed under applicable laws.

(11) No e-commerce entity shall--

(a) manipulate the price of the goods or services offered on its platform in such a manner as to gain unreasonable profit by imposing on consumers any unjustified price having regard to the prevailing market conditions, the essential nature of the good or service, any extraordinary circumstances under which the good or service is offered, and any other relevant consideration in determining whether the price charged is justified;

(b) discriminate between consumers of the same class or make any arbitrary classification of consumers affecting their rights under the Act.

5. **Liabilities of marketplace e-commerce entities. –** (1) A marketplace e-commerce entity which seeks to avail the exemption from liability under sub-section (1) of section 79 of the Information Technology Act, 2000 (21 of 2000) shall comply with sub-sections (2) and (3) of that section, including the provisions of the Information Technology (Intermediary Guidelines) Rules, 2011.

(2) Every marketplace e-commerce entity shall require sellers through an undertaking to ensure that descriptions, images, and other content pertaining to goods or services on their platform is accurate and corresponds directly with the appearance, nature, quality, purpose and other general features of such good or service.

(3) Every marketplace e-commerce entity shall provide the following information in a clear and accessible manner, displayed prominently to its users at the appropriate place on its platform:

(a) details about the sellers offering goods and services, including the name of their business, whether registered or not, their geographic address,customer care number, any rating or other aggregated feedback about such seller, and any other information necessary for enabling consumers to make informed decisions at the pre-purchase stage:

Provided that a marketplace e-commerce entity shall, on a request in writing made by a consumer after the purchase of any goods or services on its platform by such consumer, provide him with information regarding the seller from which such consumer has made such purchase, including the principal geographic address of its headquarters and all branches, name and details of its website, its email address and any other information necessary for communication with the seller for effective dispute resolution;

(b) a ticket number for each complaint lodged through which the consumer can track the status of the complaint;

(c) information relating to return, refund, exchange, warranty and guarantee, delivery and shipment, modes of payment, and grievance redressal mechanism, and any other similar information which may be required by consumers to make informed decisions;

(d) information on available payment methods, the security of those payment methods, any fees or charges payable by users, the procedure to cancel regular payments under those methods, charge-back options, if any, and the contact information of the relevant payment service provider;

(ङ) all information provided to it by sellers under sub-rule (5) of rule 6; and

(च) an explanation of the main parameters which, individually or collectively, are most significant in determining the ranking of goods or sellers on its platform and the relative importance of those main parameters through an easily and publicly available description drafted in plain and intelligible language.

(4) Every marketplace e-commerce entity shall include in its terms and conditions generally governing its relationship with sellers on its platform, a description of any differentiated treatment which it gives or might give between goods or services or sellers of the same category.

(5) Every marketplace e-commerce entity shall take reasonable efforts to maintain a record of relevant information allowing for the identification of all sellers who have repeatedly offered goods or services that have previously been removed or access to which has previously been disabled under the Copyright Act, 1957 (14 of 1957), the Trade Marks Act, 1999 (47 of 1999) or the Information Technology Act, 2000 (21 of 2000):

Provided that no such e-commerce entity shall be required to terminate the access of such seller to its platform pursuant to this sub-rule but may do so on a voluntary basis.

6. **Duties of sellers on marketplace. –** (1) No seller offering goods or services through a marketplace e-commerce entity shall adopt any unfair trade practice whether in the course of the offer on the e-commerce entity's platform or otherwise.

(2) No such seller shall falsely represent itself as a consumer and post reviews about goods or services or misrepresent the quality or the features of any goods or services.

(3) No seller offering goods or services through a marketplace e-commerce entity shall refuse to take back goods, or withdraw or discontinue services purchased or agreed to be purchased, or refuse to refund consideration, if paid, if such goods or services are defective, deficient or spurious, or if the goods or services are not of the characteristics or features as advertised or as agreed to, or if such goods or services are delivered late from the stated delivery schedule:

Provided that in the case of late delivery, this sub-rule shall not be applied if such late delivery was due to force majeure.

(4) Any seller offering goods or services through a marketplace e-commerce entity shall:

(a) have a prior written contract with the respective e-commerce entity in order to undertake or solicit such sale or offer;

(b) appoint a grievance officer for consumer grievance redressal and ensure that the grievance officer acknowledges the receipt of any consumer complaint within forty-eight hours and redresses the complaint within one month from the date of receipt of the complaint;

(c) ensure that the advertisements for marketing of goods or services are consistent with the actual characteristics, access and usage conditions of such goods or services.

(d) provide to the e-commerce entity its legal name, principal geographic address of its headquarters and all branches, the name and details of its website, its e-mail address, customer care contact details such as fax, landline, and mobile numbers and where applicable, its GSTIN and PAN details.

(5) Any seller offering goods or services through a marketplace e-commerce entity shall provide the following information to the e-commerce entity to be displayed on its platform or website:

(a) all contractual information required to be disclosed by law;

(b) total price in single figure of any good or service, along with the breakup price for the good or service, showing all the compulsory and voluntary charges such as delivery charges, postage and handling charges, conveyance charges and the applicable tax, as applicable;

(c) all mandatory notices and information provided by applicable laws, and the expiry date of the good being offered for sale, where applicable;

(d) all relevant details about the goods and services offered for sale by the seller including country of origin which are necessary for enabling the consumer to make an informed decision at the pre-purchase stage;

(e) the name and contact numbers, and designation of the grievance officer for consumer grievance redressal or for reporting any other matter;

(f) name and details of importer, and guarantees related to the authenticity or genuineness of the imported products;

(g) accurate information related to terms of exchange, returns, and refund including information related to costs of return shipping in a clear and accessible manner;

(h) relevant details related to delivery and shipment of such goods or services; and

(i) any relevant guarantees or warranties applicable to such goods or services.

7. **Duties and liabilities of inventory e-commerce entities: -**

(1) Every inventory e-commerce entity shall provide the following information in a clear and accessible manner, displayed prominently to its users:

(a) accurate information related to return, refund, exchange, warranty and guarantee, delivery and shipment, cost of return shipping, mode of payments, grievance redressal mechanism, and any other similar information which may be required by consumers to make informed decisions;

(b) all mandatory notices and information required by applicable laws;

(c) information on available payment methods, the security of those payment methods, the procedure to cancel regular payments under those methods, any fees or charges payable by users, charge back options, if any, and the contact information of the relevant payment service provider;

(d) all contractual information required to be disclosed by law;

(e) total price in single figure of any good or service along with the breakup price for the good or service, showing all the compulsory and voluntary charges, such as delivery charges, postage and handling charges, conveyance charges and the applicable tax; and

(f) a ticket number for each complaint lodged, through which the consumer can track the status of their complaint.

(2) No inventory e-commerce entity shall falsely represent itself as a consumer and post reviews about goods and services or misrepresent the quality or the features of any goods or services.

(3) Every inventory e-commerce entity shall ensure that the advertisements for marketing of goods or services are consistent with the actual characteristics, access and usage conditions of such goods or services;

(4) No inventory e-commerce entity shall refuse to take back goods, or withdraw or discontinue services purchased or agreed to be purchased, or refuse to refund consideration, if paid, if such goods or services are defective, deficient spurious, or if the goods or services are not of the characteristics or features as advertised or as agreed to, or if such goods or services are delivered late from the stated delivery schedule:

Provided that in the case of late delivery, this sub rule shall not apply if such late delivery was due to force majeure.

(5) Any inventory e-commerce entity which explicitly or implicitly vouches for the authenticity of the goods or services sold by it, or guarantees that such goods or services are authentic, shall bear appropriate liability in any action related to the authenticity of such good or service.

8. **Contravention of rules**. — The provisions of the Consumer Protection Act, 2019 (35 of 2019) shall apply for any violation of the provisions of these rules.

[F. No. J-10/3/2018-CPU]

AMIT MEHTA, Jt. Secy.

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.
MANOJ KUMAR VERMA Digitally signed by MANOJ KUMAR VERMA Date: 2020.07.23 22:00:30 +05'30'