Global opportunities for Chartered Accountants in digital economy including digital payment and Role of Chartered Accountants in enhancing GDP and making India the most powerful nation of the world.

By

CA. (Dr.) Adukia Rajkumar Satyanarayan

Author of more than 300 books & Global business, professional growth and motivational coach

Passionate to make everyone Speaker, Writer, Acquiring New Knowledge, Professional Qualifications, Growth in Business & Promotion As CEO

Member IFAC-PAIB committee 2001-2004; Member IFRS SMEIG London 2018-2020

Ex-director - SBI mutual fund, BOI mutual fund, global mediator and international arbitrator B. Com (Hons), M.Com, FCA, FCS, FCMA, LL.B, LLM(Constitution),Dip CG, MBA, Dip IFRS (UK), DLL&LW, Dip IPR, Dip in Criminology, Ph. D, Mediation ,IP(IBBI), MBF, Dip HRM, Dip Cyber Law

20+ Certificate courses; 75+ Self Development Courses

Student of: MA (Psychology), MA (Economics), PGD CSR, PGD Crime Investigation IBBI (RV) ++++++++++++++++

Ranks ALL INDIA 1st in Inter CA; 6th in CA Final; 3rd in CMA Final, 5th in Mumbai University +++

Chairman western region ICAI 1997; Council Member ICAI 1998-2016 & 2022-25

Mob: 98200 61049; Email: rajkumar@cadrrajkumaradukia.com

You may read & download my articles from my website: - www.cadrrajkumaradukia.com

"A positive mind finds opportunity in everything. A negative mind finds fault in everything."

Introduction

From barter system to Unified Payments Interface (UPI), payment systems in India have come a long way. There has been a vast change in technology. We can say that everything from study to work, from shopping to entertainment can be done with the help of internet. Today's world is digital world. In fact, from rising in the morning to going to bed we use this technology and become used to of internet.

It makes our life the easiest one. We can easily access everything at a one place. Digital economy is growing very fast. This economy provides wide range of opportunities for professionals.

Digital economy is the economic activity that involves commercial transactions and professional connections through the means of using information technologies. These activities are done globally to reach the global market. This market provides wide opportunities for Chartered Accountants to do business globally and reach global market. It gave the professionals a scope to make India a leading country in terms of economy and technology and transforming India into digital economy.

"The status that now matters is not whether we are awake or asleep, but whether we are online or offline."

-Narendra Modi

Economic development and GDP

When we look back at the history of India, India was the one of the largest economies in the world , for about two and a half millennia starting around the end of 1st millennium BC and ending around the beginning of British rule in India. The Indian economy was large and prosperous under the Mughal Empire, up until the 18th century. India has experienced highest GPD. From 1 century CE till the start of British colonisation in India in 17th century, India's GDP always varied between 25 - 35% world's total GDP. As per World Bank Data, India's GDP in the year 2020 is -7.3, in 2019 is 4.0, whereas in the year 2018 it was 6.5.

How Industry has developed in the world?

Industry has developed very fast in the last few years. The industrial revolution transformed economy from agriculture and handicrafts to industrialization. These changes based on various factors such as Business, Technology, Government and Labour. The Industrial development has had an important role in the economic growth of countries. Technological change and innovations are essential sources of structural change.

India ranks **130 on 2018 Human Development Index** out of 189 countries in the latest human development rankings by the **United Nations Development Programme (UNDP).** Between 1990 and 2017, India's HDI value incased from 0.427 to 0.640, an increase of nearly 50 percent.

Industrial Revolution

Industrial Revolution means change of handicraft economy to one dominated by industry and machine manufacturing and digital economy. The process of technological change is known as Industrial Revolution.

The process of Industrial Revolution was started in Britain in the 18th Century which was later on spread to the whole world. The word *Industrial Revolution* was first popularized by the English economic historian Arnold Toynbee (1852–83) to describe Britain's economic development from 1760 to 1830.

Industrial Revolution 1.0 (1760-1830)

- In the period 1760 to 1830 the Industrial Revolution was limited to Britain
- It was also limited to steam power and water power.

Industrial Revolution 2.0 (1870-1914)

- developments in machines, tools, and computers that gave rise to the automatic factory.
- revolved around mass production and assembly lines using electricity.
- industrial arrangement of machines, equipment, and workers for continuous flow of workpieces in mass-production operations.
- automated assembly lines consist entirely of machines run by machines,

- petroleum refining and chemical manufacture and in many modern automobile-engine plants, assembly lines are completely mechanized and consist almost entirely of automatic, self-regulating equipment.

Industrial Revolution 3.0-20th Century

- Introduction of more automated system into assembly line
- New convergence of communication and energy
- Introduction of internet
- Automation of production through electronic and Information Technology system

Industrial Revolution 4.0-early 21st Century

- Klaus Schwab, the founder of the World Economic Forum, coined the term "The Fourth Industrial Revolution" at the WEF meeting in Davos in 2016.
- growing trend towards automation and data exchange in technology and processes within the manufacturing industry, including:
    - The internet of things (IoT)
    - The industrial internet of things (IIoT)
    - Cyber-physical systems (CPS)
    - Smart manufacture
    - Smart factories
    - Cloud computing
    - Cognitive computing
    - Artificial intelligence
- Wireless connectivity and the augmentation of machines will be greatly advanced with the full roll out of 5G.
- The fourth industrial revolution also relates to digital twin technologies.
- The Internet of Things (IoT) and big data will provide information and take decisions that will help us work better and faster. This change had started in the 4IR.

Industrial Revolution 5.0- (5IR)-2nd decade of 21st century

- “Industry 5.0 will make the factory a place where creative people can come and work, to create a more personalised and human experience for workers and their customers,” says Esben Østergaard, Universal Robots chief technology officer and co-founder.
- involves robots and smart machines allowing humans to work better and smarter.
- Typewriters disappeared when word processors became ubiquitous.
- Ubiquitous meaning-present, appearing, or found everywhere.
- Networked sensors will collect data everywhere, from your smart house to autonomous manufacturing plants, to traffic in the street.
- Smart sensing will involve using the human brain as the source of signals.

Components of digital economy

1. Government: policy and regulation
2. internet, the world wide web (WWW)
3. electricity infrastructure
4. telecommunication industry
5. digital service providers
6. e-business and e-commerce industry
7. information and knowledge management systems
8. intellectual property rights
9. human capital and knowledge workers
10. research and development
11. emerging technologies
12. digital payment

What is e-commerce?

It is business model that allows companies and individuals to buy and sell goods and services over the Internet. It is also known as electronic commerce or internet. As the transaction is done through the internet or electronic means so, it is termed as e-commerce.

E-commerce History-year wise

- 1969: CompuServe is founded by electrical engineering students Dr. John R. Goltz and Jeffrey Wilkins- https://www.compuserve.com/

  In 1979, CompuServe became the first service to offer electronic mail capabilities and technical support to personal computer users.

  Launch of CompuServe 7.0 in 2001

- 1979: Michael Aldrich invents electronic shopping. -
- 1982: Boston Computer Exchange launches- world's first ecommerce company.
- 1992: Book Stacks Unlimited launches as first online book marketplace.
- 1994: Netscape Navigator launches as a web browser-by Marc Andreessen and Jim Clark
- During the 1990s, Netscape Navigator became the primary web browser on the Windows platform, before the rise of modern giants like Google.
- 1998: PayPal launches as an ecommerce payment system.
- 1999: Alibaba launches.
- 2000: Google introduces Google AdWords as an online advertising tool.
- 2004: Shopify launches.
- 2005: Amazon introduces Amazon Prime membership.
- 2005: Etsy launches.
- 2009: BigCommerce launches- Eddie Machaalani and Mitchell Harper co-founded BigCommerce
- 2011: Google Wallet introduced as a digital payment method- peer-to-peer payment service
- Today, Google Wallet has joined with Android Pay for what is now known as Google Pay.
- 2011: Facebook rolls out sponsored stories as a form of early advertising.
- 2011: Stripe launches- Stripe is a payment processing company built originally for developers. It was founded by John and Patrick Collison.
- 2014: Apple Pay introduced as a mobile payment method.
- 2014: Jet.com launches- for longer shipping times and bulk ordering.
- 2017: Shoppable Instagram is introduced.
- **2020: COVID-19 Drives Ecommerce Growth- By May of 2020, ecommerce transactions reached $82.5 billion — a 77% increase from 2019.**

Activities of E-Commerce:

1. Online store setup
2. Customer education
3. Buying and selling product
4. Monetary business transaction through internet banking
5. Email marketing
6. Supply Chain Management
7. Payment gateways
8. Online ticketing

Types of electronic commerce

There are three main types of e-commerce:

A. Business-to-Business (websites such as Shopify), (B to B)-

B 2 B companies-

i. IndiaMart- https://www.indiamart.com/

Established in the year 1996, by Dinesh and Brijesh Agrawal, with a spawning capital of ₹ 40,000 now IndiaMart is the most popular Indian B2B eCommerce marketplace holding60% market share of the online B2B Classified space in the country.

ii. TradeIndia- https://www.tradeindia.com/

TradeIndia is also one of top India originated portals, established in the same year as Indiamart. This ecommerce business was started by Bikky Khosla who is presently the chairperson of the eCommerce committee in India.

iii. **TradekeyIndia- https://www.tradekeyindia.com/**

It is a b2b portal, having its registered office in Delhi. It has more than 2 million registered users.

iv. **Udaan- https://udaan.com/**

It was founded by former Flipkart employee Sujeet Kumar, Amod Malviya, and Vaibhav Gupta. It is headquartered in Bengaluru Udaan has a network of over 3 million registered users and 25,0000-30,000 sellers across 900+ cities in the country covering more than 12,000 pin codes.

v. **Alibaba- https://www.alibaba.com/**

It is a Chinese multinational company specializing in e-commerce, retail, Internet, and technology. Founded by Jack Ma the principal co-founder.

vi. **ExportsIndia- https://www.exportersindia.com/**

It was founded in 1997 by Sunil Kumar Gupta.

vii. **DHgate- https://www.dhgate.com/**

The world's leading online marketplace for wholesale consumer products. Its partners include American Express, DHL, FedEx, MasterCard, Visa, UPS. It is Founded by Diane Wang and is CEO of DHgate.com. Before founding DHgate, Ms. Wang co-founded and served as CEO of Joyo.com, which at the time was the largest B2C (Business-to-Consumer) online marketplace in China.

viii. **99 business.Com – http://www.99business.com/**

Unique B2B Portal For Business Success and Growth. This was Founded by Mr. Diago Silveira. It is a free registration and no need to pay even a single penny.

ix. **Go4worldbusiness- https://www.go4worldbusiness.com/**

Go4worldbusiness is an online B2B marketplace for connecting global manufacturers, importers and exporters. Krishna Kant Bhatt is the director of go4worldbusiness.

x. **Global Trade Bazaar- https://www.globaltradebazaar.com/**

Global Trade Bazaar, is a B2B Portal, which helps the buyers and suppliers connect all over the world. Global Trade Bazar is managed by the Webecom Media Pvt Ltd.

B. Business-to-Consumer (websites such as Amazon), (B to C)

i. Amazon -https://www.amazon.in/

It is an American multinational technology company which focuses on e-commerce, cloud computing, digital streaming, and artificial intelligence.

Amazon India launched operations in June 2013. The company launched its website Amazon.in. Amazon India is a fully-owned subsidiary of US based e-commerce giant Amazon, Inc. The parent company Amazon was founded in 1994 by Jeff Bezos.

ii. Walmart-https://www.walmart.com/

Wal-Mart was founded by Sam Walton in Rogers, Arkansas, in 1962.

iii. Netflix-https://www.netflix.com/in/

Netflix, Inc. is an American subscription streaming service and production company. Launched on August 29, 1997.

v. **Flipkart-https://www.flipkart.com/**

It is an ecommerce company, founded in 2007.and has headquarters in Bengaluru, Karnataka, India.

vi. **Snapdeal- https://www.snapdeal.com/**

It was founded in 2010, having its headquarters in Gurugram, Haryana, India. Snapdeal is founded by Rohit Bansal and Kunal Bahl.

vii. **Nykaa- https://www.nykaa.com/**

It was founded in 2012 by Falguni Nayar.

viii. **Myntra- https://www.myntra.com/**

Myntra Jabong was founded in 2007, having its headquarters in Bengaluru, Karnataka, India. It is founded by Mukesh Bansal.

ix. **LimeRoad- https://www.limeroad.com/**

Limeroad.com is a Fashion & Apparel company and has headquarters in Gurugram, Haryana, India. It was founded in 2012 by Ankush Mehra, Manish Saksena, Prashant Malik and Suchi Mukherjee.

x. **Shopify-https://www.shopify.in/**

Shopify was founded in 2006 by Tobias Lütke and Scott Lake. It is an ecommerce company based in Ottawa, Ontario, Canada.

C. **Consumer-to-Consumer (websites such as eBay). (C to C)**

i. **ebay- https://www.ebay.com/**

It was founded in 1995 by Pierre Omidyar. The Company deals with electronic accessories, mobiles, apparels, and beauty products.

ii. **OLX- https://www.olx.in/**

It was founded in 2006 by Fabrice Grinda ("Grinda"), Alec Oxenford ("Oxenford"), and Jordi Castello ("Castello"). In India it was launched in 2009. It deals with 20+ Brands.

iii. **Quikr- https://www.quikr.com/**

It was founded by Pranay Chulet and Jiby Thomas in 2008.It is a platform where we can sell, buy, rent or find anything.

Other E-commerce companies

1. **Amazon Development Centre India Pvt. Ltd.- https://www.amazon.in/**

Amazon.com, Inc. often referred to as simply Amazon is American electronic commerce and cloud computing company with headquarters in Seattle Washington.

2. **Grofers India Pvt. Ltd.- https://blinkit.com/**

   "Blinkit (formerly Grofers)" is owned & managed by "Grofers India Private Limited"

   Grofers was founded in the year 2013 by Saurabh Kumar and Albinder Dhindsa. The leading online grocery delivery platform is headquartered in Gurgaon, Haryana.

3. **Just Dial Ltd.- https://www.justdial.com/**

   Just Dial Limited is India's No. 1 Local Search engine that provides local search related services to users across India through multiple platforms such as website, mobile website, Apps (Android, iOS), over the telephone (voice, pan India number 8888888888) and text (SMS).

   The company's operations began in 1996, The officialwebsite www.justdial.com was launched in 2007

4. **MakeMyTrip Ltd.- https://www.makemytrip.com/**

   MakeMyTrip is an Indian online travel company founded in 2000. Headquartered in Gurugram, Haryana, the company provides online travel services including airline tickets, domestic and international holiday packages, hotel reservations, rail, and bus tickets.

5. **Myntra Designs Pvt. Ltd.- https://www.myntra.com/**

   The original B2B venture for personalized gifts was conceived in 2007 but transitioned into a full-fledged ecommerce giant within a span of just a few years. By 2012, Myntra had introduced 350 Indian and international brands to its platform, and this has only grown in number each passing year.

Technical terms related to digital economy

1. **Cyber-** The word cyber means and relates to the culture of computers, information technology, and virtual reality. It is relating to, or involving computers or computer networks (such as the Internet)
2. **Cyberspace**- It simply means the environment Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer subnetworks that is used for data exchange activities.
3. **Cyber Security** is the measures to protect our system from cyber-attacks and malicious attacks.
4. **Network security**- is a broad term that covers a multitude of technologies, devices and processes.
5. **Botnet-** A botnet is a network of devices that has been infected with malicious software, such as a virus. Attackers can control a botnet as a group without the owner's knowledge with the goal of increasing the magnitude of their attacks. Often, a botnet is used to overwhelm systems in a distributed-denial-of-service attack (DDoS) attack.
6. **Malware-** is intrusive software that is designed to damage and destroy computers and computer systems.
7. **Antivirus** – software that scans a device or a network to detect security threats, alert you, and neutralize malicious code. Like Norton, McAfee, Kaspersky, Bitdefender, Webroot,
8. **Blacklist** – a list of emails or other service providers that spread spam messages. Blacklists help users and companies to prevent the flood of unwanted messages.
9. **Backup** – a copy of physical or virtual data so in case they are being deleted or lost user could easily recover it. Works as a part of a data loss prevention plan. Like- Google workspace backup, WhatsApp backup.
10. **Breach**- The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.
11. **Cloud –** computing recourses that make it available to access your files and services through the internet from any point in the world. It is possible thanks to a network of computers that provide storage and computing capabilities by the request.

12. **Data Loss Prevention (DLP)** – the complex of security measures, related to detecting and preventing data loss and cyberattacks. DLP is included in the organization policy, but individuals must also use this strategy to keep all data safe during ransomware or malware attack.
13. **Data encryption** – a way to secure private information by encoding it so no third parties could watch or access it. To read the encoded (encrypted) file, you must decode it by using a decryption key.
14. **Exploit –** a weak spot in a computer system, which can be used to attack this system.
    A malicious application or script that can be used to take advantage of a computer's vulnerability.
15. **Firewall** – a network security system that filters unsanctioned incoming and outgoing traffic. A network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
16. **IP Address** – IP stands for Internet Protocol. It is a unique address that identifies a device on the internet or a local network.
    It is an address that identifies the connection between our computer and the network provider. Our computer can have multiple IP addresses depending on the number of networks it connects to. Also, multiple computers can have one IP address if they are connected to the same provider in the same area, like in cafes or at home.
17. **Identity check –** a set of actions (a password, a fingerprint, or a face scan) designed for verification of someone's identity.
18. **Insider threat** – a threat to the company's data integrity that is coming from someone within the organization, usually an employee or another insider.
19. **Open Source** – a type of free technology which copyright allows using its source code for different purposes, such as studying, modifying, distributing. Examples of open-source code are Bitcoin, Mozilla Firefox, Joomla, WordPress.
20. **ReCAPTCHA –** a system invented by Google that uses a Turing test to establish if a user is a human or a robot. It is used by websites to prevent bots from spamming.
21. **Software-** A set of programs that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. For example, Microsoft Office is an application software.

22. **Domain**- A group of computers, printers and devices that are interconnected and governed as a whole. For example, your computer is usually part of a domain at your workplace. Like- http://www.. It should be purchased. Like we do company registration, likewise- Doman name should be available. A domain name is a website name.
23. **Virtual Private Network (VPN) –**It is a technology that extends a private network and all its encryption, security, and functionality across a public network. With it, users can send and receive messages as if they were connected to a private network. VPNs are a program or app that allow us to use the internet via secure, encrypted tunnels. It is an encrypted connection over the Internet from a device to a network. VPN is installed in router.
24. **Router**- A router is a networking device that forwards data packets between computer networks.
25. **Adware** – Software that automatically displays or downloads material when a user is offline.
26. **DDoS (denial-of-service attack)** – a type of cyber attack that makes the site user wants to visit unusable by flooding it with malicious traffic.
27. **Ransomcloud** – a special type of ransomware, designed to encrypt cloud emails and attachments.
28. **Rootkit** – a type of malware that is used to seep into the system and steal company information.
29. **Spyware** – malware that spies on the computer to collect information about a product, a company, a person.
30. **Trojan** – A form of malicious code that looks like a legitimate file, program, or application, but actually is designed to control the user's computer and data. It is usually hard to detect until the damages and losses are significant.
31. **Virus** – a type of malware that is aimed to infect and harm a file, a system, or a network.
32. **Worm** – a type of self-replicating malware that, when infected on a computer, is aimed to spread across the network to infect others. Worms come through system vulnerabilities or clicking on malicious attachments.
33. **Account Hijacking** – a type of identity theft, when a hacker hacks and steals someone's account to perform malicious actions.

34. **Phishing** – a wide range of scams when someone impersonates themselves as trustworthy entities in an attempt to obtain information. For example, a user can receive an email from "Google" asking them to click the link and type their login and password, or credit card information in the empty fields.
35. **Password Sniffing** – It is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords.
36. **Social Engineering –** a set of means intended to trick people into giving out sensitive information like banking and credit card details, personal information. Criminals impersonate themselves as someone trustworthy and use the seemingly legitimate pretext to make a user share data
37. **Wi-fi- Wireless Fidelity**- wireless network protocol that establishes a data transfer or Internet connection.

Digital Profile of India

- Aadhaar- 123 crore
- Mobile Phones-120 crore
- Internet Subscriptions- 49 Crore
- Common Service Centres (CSCs)- 3.12 Lakh
- There are more than 19,000+ e-commerce companies in India and over 28,000+ e-commerce companies in the United States.

Laws related to data protection in India

The Information Technology Act, 2000- notified on [9*th June*, 2000.] and came into force w.e.f. 17th October, 2000

Various rules framed under the Information Technology Act, 2000

1. The Information Technology (Certifying Authorities) Rules, 2000
2. The Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003
3. The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009
4. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
5. The Information Technology (Guidelines for Cyber Café) Rules, 2011
6. The Information Technology (Intermediaries guidelines) Rules, 2011
7. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
8. The Information Technology (Electronic Service Delivery) Rules, 2011
9. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013
10. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Various regulations framed under the Information Technology Act, 2000

1. The Information Technology (Certifying Authorities) Regulations, 2001
2. The Information Technology (Recognition of Foreign Certifying Authorities operating under a Regulatory Authority) Regulations, 2013

Contents

- 13 chapters, 90 sections and 2 schedules
- Earlier 94 sections and 4 schedules
- 4 sections 91-94 were omitted and 2 schedules i.e. 3rd and 4th schedules are omitted

Chapter I: Preliminary (Section 1 to 2)

Chapter II: Digital Signature and Electronic Signature (Section 3 & 3A)

Chapter III: Electronic Governance (Sections 4 to 10A)

Chapter IV: Attribution Acknowledgment and Dispatch of Electronic Records (Sections 11 to 13)

Chapter V: Secure Electronic Records and Secure Electronic Signatures (Sections 14 to 16)

Chapter VI: Regulation of Certifying Authorities (Sections 17 to 34)

Chapter VII: Electronic Signature Certificates (Sections 35 to 39)

Chapter VIII: Duties of Subscribers (Sections 40 to 42)

Chapter IX: Penalties Compensation and Adjudication (Sections 43 to 47)

Chapter X: The Cyber Appellate Tribunal (Sections 48 to 64)

Chapter XI: Offences (Sections 65 to section 78)

Chapter XII: Intermediaries Not To Be Liable In Certain Cases (Section 79)

Chapter XIIA: Examiner of Electronic Evidence (Section 79A)

Chapter XIII: Miscellaneous (Sections 80 to 90)

Who is the minister for information technology?

Ministry of Electronics and Information Technology- meity.gov.in

Definitions under Section 2

Asymmetric cryptosystem: An *asymmetric cryptosystem* is one where different keys are employed for the operations in the cryptosystem (e.g., encryption and decryption), and where one of the keys can be made public without compromising the secrecy of the other key.

Communication device means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

Cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is

being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer

Electronic form with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

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

Encryption is a means of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the information. It is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information.

There are two types of encryptions- symmetric and asymmetric encryption.

Information- includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer-generated micro fiche

Secure system means computer hardware, software, and procedure that–
(a) are reasonably secure from unauthorized access and misuse;
(b) provide a reasonable level of reliability and correct operation;
(c) are reasonably suited to performing the intended functions; and
(d) adhere to generally accepted security procedures

Key pair- Key pair, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

Electronic and digital signature

Digital signature as per section 2 (p) means authentication of any electronic record by a subscriber by means of an electronic method

Electronic signatures include all forms of a signature whereas digital signatures are attached to an actual signature.

Electronic signature and digital signature are different. The key differences are: Digital signature is used to secure a document while an electronic signature is used to verify a document.

As per Section 3A, a subscriber has an option to authenticate any electronic record by such electronic signature or electronic authentication technique which is reliable and given under second schedule of this Act.

Legal recognition of electronic records (Section 4)

If any law requires that the information or any other matter either in writing or in the typewritten or printed form, then such information or matter is required to be–

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

Legal recognition of electronic signatures (Section 5)

Where there is a requirement in any law that the document should be signed or bear the signature of any person, then such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature] affixed in such manner as may be prescribed by the Central Government.

Various use of electronic records and electronic signatures in Government and its agencies (Section 6)

(*a*) the filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner

(b) the issue or grant of any licence, permit, sanction or approval

(c) the receipt or payment of money

Delivery of services by service provider (Section 6A)

Here service provider includes-

- any individual,
- private agency,
- private company,
- partnership firm,
- sole proprietor firm or
- any such other body or agency

which has been granted permission by the Government to offer services through electronic means.

In order to make the efficient delivery of services to the public through electronic means, the Government may give the permission to set up, maintain and upgrade the computerised facilities and to perform other services.

Audit of documents, etc., maintained in electronic form (Section 7A)

Where any law provides for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in the electronic form.

What is the validity of contracts formed through electronic means?

Section 10 A provides that when the contract is formed via electronic means such as the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall be treated as same as in physical case. It cannot be refused only on the grounds that it is made through electronic means.

CERTIFYING AUTHORITIES- (Sections 17- 34)

The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Information Technology Act, 2000.

The Office of the CCA came into existence on November 1, 2000.

https://cca.gov.in/

License to issue electronic signature Certificates

As per Section 22, any person may make an application, to the Controller, for a licence to issue electronic signature Certificates provided that every application for issue of a licence shall be accompanied by—

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government

Certifying Authorities

Certifying Authorities has been granted a license to issue a digital signature certificate under Section 24 of the Information Technology Act, 2000. There are Class 2 or 3 certificates which can be issued from any of the certifying authorities.

1. Safescrypt

2. IDRBT

3. (n)Code Solutions

4. e-Mudhra

5. CDAC

6. Capricorn

7. NSDL e-Gov

8. Vsign (Verasys)

9. Indian Air Force

10. CSC

11. RISL (RajComp)

12. Indian Army

13. IDSign

14. CDSL Ventures

15. Panta Sign

Functions of controller

The Controller may additionally carry out all or any of the following functions:

1) Supervises the activities of Certifying Authorities.

2) Certifies public keys of the Certifying Authorities.

3) Drafts the requirements to be maintained by way of Certifying Authorities.

4) Specifies the qualifications and revel in of employees of the Certifying Authorities.

5) Specifies the situations below which the Certifying Authority shall conduct their business;

6) Specifies the contents of written, revealed or visual materials and commercials that may be distributed or utilized in a Digital Signature Certificate and the general public key;

7) Specifies the format and content of a Digital Signature Certificate and the important thing;

8) Specifies the layout wherein Certifying Authorities shall keep the bills.

9) Specifies the terms and situations for the appointment of the auditors and their remuneration.

10) Helps the Certifying Authorities in organizing any digital machine and law of such gadget.

11) Specifies the way wherein the Certifying Authorities shall address the subscribers.

12) Resolves any warfare that arises between the Certifying Authorities and the subscribers;

13) Lays down the duties of the Certifying Authorities;

14) Maintains a database containing the disclosure record of ever Certifying Authority.

15) Maintains the database of public keys in a way that it is available to the general public.

16) Issues the license to issue the Digital Signature Certificate.

17) Can suspend the license if he isn't pleased with the validity of the applicant.

Disclosure to be made by Certifying Authority

Every Certifying Authority is required to disclose the following-

(a) its electronic signature Certificate

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a electronic signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

"Cyber Regulation Advisory Committee", consisting of the following, namely: -

1.Minister, Information Technology Chairman

2. Secretary, Legislative Department Member

3. Secretary, Ministry of Information Technology Member

4. Secretary, Department of Telecommunications Member

5. Finance Secretary Member

6. Secretary, Ministry of Defence Member

7. Secretary, Ministry of Home Affairs Member

8. Secretary, Ministry of Commerce Member

9.Deputy Governor, Reserve Bank of India Member

10. Shri T K Vishwanathan, Presently Member Secretary, Law Commission Member

11. President, NASSCOM Member

12. President, Internet Service Providers Association Member

13. Director, Central Bureau of Investigation Member

14. Controller of Certifying Authority Member

15. Information Technology Secretary by rotation from the States Member

16. Director General of Police by rotation from the States Member

17. Director, IIT by rotation from the IITs Member

18. Representative of CII Member

19. Representative of FICCI Member

20. Representative of ASSOCHAM Member

21. Senior Director, Ministry of Information Technology Member Secretary

Penal Provisions under Chapter IX

Sl. No.	Provision	Penalty
1	Penalty and compensation for damage to computer, computer system, etc.–	liable to pay damages by way of compensation to the person so affected
2	Compensation for failure to protect data	liable to pay damages by way of compensation to the person so affected
3	Penalty for failure to furnish any document, return or report to the Controller or the Certifying Authority	liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure
4	Penalty for failure to file any return or furnish any information, books or other documents within the time specified	liable to a penalty not exceeding five thousand rupees for every day during which such failure continues
5	Contravention of any rules or regulations made under this Act not for which penalty is not specifically mentioned	liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Appellate Tribunal

The Appellate Tribunal for the purpose of Information Technology Act, 2000 is the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997. Earlier, Cyber Appellate Tribunal was the appellate tribunal for the same purpose. It was *Omitted by the Finance Act*, 2017 and replaced by the Telecom Disputes Settlement and Appellate Tribunal w.e.f. 26.05.2017.

Powers of the Appellate Tribunal

The following are the powers of the Appellate Tribunal-

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it ex parte;

(g) any other matter which may be prescribed.

Appeal to High Court.

Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Appellate Tribunal to him on any question of fact or law arising out of such order

Draft Data Protection Bill, 2021

Introduced on: 11th December 2019

Draft report presented on: 16th December, 2021

The importance of data protection has been recognized by our country and therefore, the Personal Data Protection Bill, 2019 that was first introduced in Lok Sabha on 11th December, 2019. Then the bill was moved to a Joint committee of both Houses of Parliament. The committee then held 3 benefiting meetings till now and presented the draft report on 16th December, 2021.

This report is divided into 2 Parts. Part-I deals with the data protection and privacy. Part- II provides clause by clause examination on "the Personal Data Protection Bill, 2019." It contains an annexure which provides for the bill as reported by the Joint Committee. It aims to protect privacy of individuals by regulating how their data can be used and processed. It aims to provide for protection of the digital privacy of individuals.

The committee recommended to amend the title of the Bill from the Personal Data Protection Bill, 2019 to the Data Protection Bill, 2021 as it is not possible to segregate the personal and non-personal data at every stage. The bill now deals with both personal and non-personal data.

Brief background of the bill

- At first, in August 2017, a nine-judge bench of the Supreme Court in Justice K. S. Puttaswamy (Retd) Vs Union of India unanimously held that Indians have a constitutionally protected fundamental right to privacy that is an intrinsic part of life and liberty under Article 21. This gives rise to the formation of committee to study issues related to data protection.
- Following this, the Ministry of Electronics and Information Technology set up a committee to study issues related to data protection. The committee was chaired by retired Supreme Court judge Justice B. N. Srikrishna..
- The committee submitted the draft Personal Data Protection Bill, 2018 on 27 July 2018 followed by introduction of personal data protection bill 2019 on 11th dec 2019 in parliament
- The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same.

- Then Krish Gopalakrishnan has given report in July 2020 on non-personal data protection
- Then, the Joint Parliamentary Committee presented the draft report on 16th December, 2021 i.e., the Data Protection Bill, 2021.

Contents

This bill contains 14 Chapters, 99 Clauses and a Schedule.

Chapter-1- Preliminary- Clauses-1 to 3

Chapter- II- Obligations of data fiduciary-Clause- 4 to 11

Chapter-III- Grounds for Processing of Personal Data without Consent- Clause- 12 to 15

Chapter- IV- Personal Data of children- Clause- 16

Chapter V- Rights of Data Principal Clause- 17 to 22

Chapter- VI- Transparency and Accountability Measures- Clause- 23 to 32

Chapter- VII- Restriction on Transfer of Personal Data Outside India- Clause- 33-34

Chapter- VIII- Exemptions- Clause- 35 to 40

Chapter- IX- Data Protection Authority of India- Clause- 41 to 56

Chapter- X- Penalties and Compensation- Clause- 57 to 67

Chapter- XI- Appellate Tribunal- Clause- 68 to 78

Chapter- XII- Finance, Accounts and Audit- Clause- 79 to 82

Chapter- XIII- Offences- Clause- 83 to 86

Chapter- XIV- Miscellaneous- Clause- 87 to 99

Salient features of the Bill-

- ✓ It has discussed the importance of protecting the right to data portability from frivolous claims of trade secrets that may be used to deny data portability.
- ✓ It imposed an obligation on data fiduciaries to inform the Data Protection Authority within 72 hours.
- ✓ The permission has been granted to the Data Protection Authority to categorize those data fiduciaries that deal with the processing of data related to children as significant data fiduciaries.
- ✓ The JPC Report also recommended that all social media platforms which do not act as intermediaries be treated as publishers and be held accountable for the content they host.
- ✓ Data Protection Authority of India shall be the Adjudicating Authority
- ✓ As per Clause 3 (7) of the Bill, biometric data means facial images, fingerprints, scans or any other similar personal data resulting from measurements or technical processing, operations carried out on physical, physiological or behavioral characteristics of data principal, which allow or confirm the unique identification of that natural person.
- ✓ This bill also defines data auditor
- ✓ Data breach includes both personal as well as non-personal data breach.
- ✓ Data fiduciary includes- a State, Company a non-government organization, juristic entity, or any individual either alone or together with others determines the purpose and means of processing of personal data.
- ✓ Data processor- includes- a State, Company a non-government organization, juristic entity, or any individual who processes personal data on behalf of data fiduciary.
- ✓ Data protection officer- officer appointed by the data fiduciary.
- ✓ Section- 99- amendment in the Information Technology Act, 2000 as per schedule
- ✓ Schedule- amendment in section 43A of the Information Technology Act, 2000 - omitted
- ✓ Section 43A of the Information Technology Act, 2000 deals with Compensation for failure to protect data, it is omitted

- ✓ Social media platform includes those platforms which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.
- ✓ This bill prescribes limitation on collection of personal data, requirement of notice for collection of personal data, restriction on retention of personal data, accountability of data fiduciary.
- ✓ Clause 13 deals with the processing of personal necessary for purposes related to employment.
- ✓ Clause 14 provides processing of personal data for other reasonable purposes.
- ✓ Clause 16 provides that it is the duty of the data fiduciary to process the personal data of the child in such manner that protects the right of the child.
- ✓ Chapter V provides the right of data principal i.e. the right to confirmation and access, right to correction and erasure, right to data portability, right to be forgotten.
- ✓ Clause 22 provides that it is the duty of the data fiduciary to prepare a privacy by disg policy which includes the managerial, organizational, business practices, and technical systems, designed to anticipate; its obligations; technology used in the processing of personal data; the protection of privacy.
- ✓ It is the duty of the data fiduciary to maintain transparency, security safeguards in processing of personal data, reporting of data breach, maintenance of records, audit of policies, and conduct of processing by an independent data auditor.
- ✓ The data fiduciary shall appoint a data protection officer for providing information, monitoring data processing activities providing assistance to authority on matters of compliance, providing advice to data fiduciary on various matters, maintain records and acts as a point of contact for the data principal.
- ✓ Chapter VII of the bill provides various restrictions on transfer of personal data outside India such as prohibition on processing of sensitive personal data and critical personal data.
- ✓ Chapter VIII deals with exemptions for Government Departments by the insertion of a non-obstante provision in Clause 35
- ✓ Chapter IX delas with the establishment of Data Protection Authority, its composition and qualifications, terms and conditions of the appointment of Data Protection

Authority i.e. the Chairperson and members of the authority shall be appointed for a terms of five years and not eligible for re-appointment.

- ✓ The authority must follow the code of practice during their tenure of the office.
- ✓ This bill deals with various penal provisions under Chapter X.

General Data Protection Regulation (GDPR)- https://gdpr.eu/

The General Data Protection Regulation (EU) (GDPR) is a regulation on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).

The General Data Protection Regulation was adopted on 14 April 2016. The regulation was put into effect on May 25, 2018 . As the General Data Protection Regulation is a regulation, not a directive, it is directly binding and applicable, but does provide flexibility for certain aspects of the regulation to be adjusted by individual member states.

Background

The right to privacy is part of the 1950 European Convention on Human Rights, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence." From this basis, the European Union has sought to ensure the protection of this right through legislation.

As technology progressed and the Internet was invented, the European Union recognized the need for modern protections. So, in 1995 it passed the European Data Protection Directive, establishing minimum data privacy and security standards, upon which each member state based its own implementing law. The General Data Protection Regulation entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant with this regulation.

Contents

It contains 11 chapters and 99 Articles.

Various terms defined:

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;

'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

'Supervisory authority' means an independent public authority which is established by a Member State

Salient features of the General Data Protection Regulation -

- The controller shall be responsible for, and be able to demonstrate compliance with.

- Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

- Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.
- The Commission shall be empowered to adopt delegated acts for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.
- The controller has the right to lodge a complaint with a supervisory authority.

About Various Ministries and Regulatory Authorities in digital economy

1. **Ministry of Electronics and Information Technology- https://www.meity.gov.in/**

   The Ministry of Electronics and Information Technology is the minister for information technology in India. It is the responsibility of the Ministry of Electronics & Information

Technology (MeitY) to encourage initiative on "Promotion of Digital Transactions including Digital Payments" in India.

2. **Digital Economy & Digital Payment Division (DEDPD)-** It is a division created under the Ministry of Electronics & Information Technology for making available digital governance and digital services to every citizen. 'Digidhan Mission' has been set up for building strategies and approaches in collaboration with all stakeholders to promote digital payments and create awareness.

   In order to promote digital transactions in India, the Ministry of Electronics & Information Technology has taken various initiatives such as-

   (a) Digital payment transactions target has been assigned to Central Ministries with high citizen touch points, Public Sector and Private Sector Banks to achieve the target as announced in the Budget speech for FY 2017-18.

   (b) Various Training and workshops on digital payments awareness with several Ministries have been conducted together with other ministries. Such as-Ministry of Road Transport and Highways,

   Ministry of Health and Family Welfare, Ministry of Agriculture, MSME, Department of Post, Ministry of Power, Panchayti Raj, Ministry of Defense

   (c) Digital Payment dash board has been created to track and monitor the progress of digital transactions achieved by Banks

   (d) Promotion and awareness approach framework on digital payments has been shared with Banks

   Various schemes issued are-

   a) BHIM cash back schemes for merchants
   b) BHIM Aadhaar merchant incentive schemes
   c) BHIM referral bonus schemes for Individuals

Ministries Promoting Digital Payments

List of Union Ministries and Departments

S.No.	Ministry/Departments
1.	Ministry of Road Transport and Highways
2.	Ministry of Communications
3.	Ministry of Railways
4.	Ministry of Petroleum and Natural Gas
5.	Ministry of Human Resource Development
6.	Ministry of Power
7.	Ministry of Agriculture
8.	Dept. of Posts
9.	Ministry of Health and Family Welfare
10.	Ministry of Consumer Affairs, Food & Public Distribution
11.	Ministry of Rural Development
12.	Department of Animal Husbandry
13.	Department of Fertilizers
14.	Ministry of Culture
15.	Ministry of Urban Development
16.	Ministry of Home Affairs
17.	Ministry of Tourism

List of Union Ministries and Departments

S.No.	Ministry/Departments
18.	Ministry of Labour
19.	Ministry of Panchayati Raj
20.	Ministry of Drinking water & Sanitation
21.	Department of Defence
22.	Ministry of Civil Aviation
23.	Ministry of MSME
24.	Department of Heavy Industries
25.	Department for Financial Services (non-banks)
26.	Ministry of Women & Child Development
27.	Ministry of Environment, Forest & Climate Change
28.	Department of Ex Serviceman welfare
29.	Ministry of External Affairs
30.	Ministry Skill Development & Entrepreneurship
31.	Ministry of Steel
32.	Ministry of Youth Affairs and Sports
33.	Ministry of Home Affairs
34.	Ministry of Urban Development
35.	Ministry of Electronics and Information Technology

3. The Telecom Regulatory Authority of India (TRAI)- https://www.trai.gov.in/

On 16th December, 2021, the Telecom Regulatory Authority of India issued a consultation paper on 'Regulatory Framework for Promoting Data Economy Through Establishment of Data Centers, Content Delivery Networks, and Interconnect Exchanges in India'. It is open for stakeholders written Comments and Counter Comments up to 3rd February, 2022 and 17th February,2022 respectively.

The main aim behind this consultation paper is 'CPS'i.e.-

1) Connect India: Creating robust digital communications infrastructure to promote 'Broadband for All' as a tool for socio-economic development.

2) Propel India: To harness the power of emerging digital technologies, including 5G, AI, IoT, Cloud, and Big Data to enable the provision of future-ready products and services; and to catalyze the fourth industrial revolution (Industry 4.0) by promoting Investments, Innovation and IPR generation.

3) Secure India: To secure the interests of citizens and safeguard the digital sovereignty of India with a focus on ensuring individual autonomy and choice, data ownership, privacy, and security, while recognizing data as a crucial economic resource.

This paper contains 6 chapters and 3 annexures and provides 7 tables.

Chapter 1- Introduction

Chapter 2- Data Centers

Chapter 3- Content Delivery Networks

Chapter 4- Interconnect Exchanges

Chapter 5- Data Ethics — Privacy, Ownership, and Security

Chapter 6- Issues for Consultation

Defining the terms

Data Centres- Data centres are physical facilities used to host data and applications.

Content Delivery Networks- It is a system consisting of a distributed group of servers and networks.

Interconnect Exchange Point- is a technical facility to route traffic quickly and cost-effectively between network members by enabling interconnection.

Digital economy- As per the Organization for Economic Co-operation and Development, "The Digital Economy incorporates all economic activity reliant on, or significantly enhanced by the use of digital inputs, including digital technologies, digital infrastructure, digital services, and data. It refers to all producers and consumers, including Government, that are utilizing these digital inputs in their economic activities".

Data Centre Parks- These are the specialized secure Data Zone, strategically located with the most conducive non-IT and IT infrastructure, and regulatory environment for housing a mix of small scale/large scale clusters of Data Centres to serve the high needs of compute, storage, networking, and provision of a wide range of data-related services.

Data ethics are inter-personal, social, organisational, and national norms that govern how people/data users should conduct and behave in the digital world.

Various recommendations of the Telecom Regulatory Authority of India-

- to formulate reliable frameworks and policies to encourage development of 5G, Internet of Things, Data Centers, and associated services, data analytics, edge computing, digital platforms, and applications.

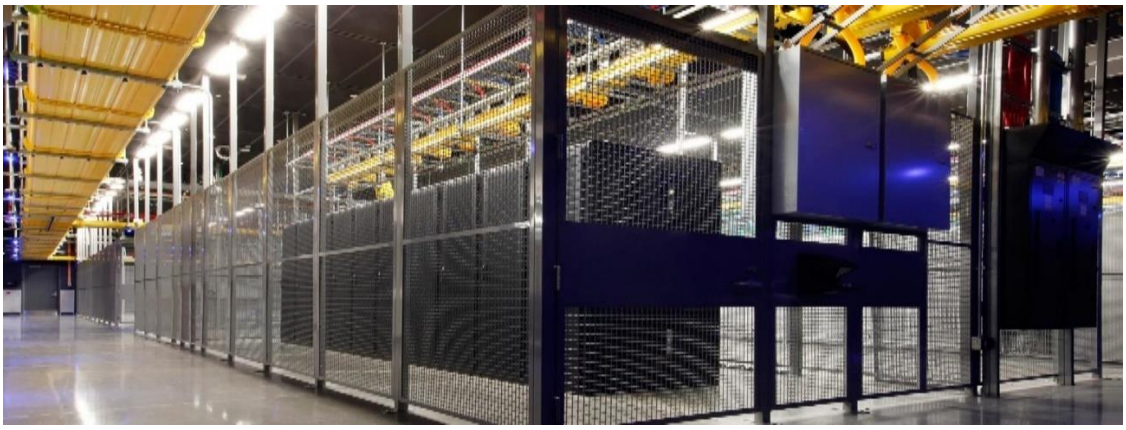
- To set up infrastructure for digital ecosystem and facilities include:

- Data Centres – used for edge computing, hosting of content, and delivering cloud-based services,
- Content Delivery Networks – used for delivering the content from the cloud to the edge of the network, and
- Internet Exchange Points – enables networks to exchange traffic with each other in the internet infrastructure.

- Promoting data centres and data parks
- These are the building blocks of data centre-server, network and building area.
- TRAI finds the four most critical aspects in establishing data centres are Land, Power, Telecom and IT Element/Networks and Ease of Doing business. These includes capital expenditure and operational expenditure such as cost of broadband connectivity, cost of power for equipment operation, as well as for cooling, repairs, and annual expenditures like wages for employees.
- Internal and external audit for data centres.
- Various challenges in establishing data centres- capacity building, Centre-State Coordination, Edge Data and AI-enabled Data Centre, Data digitization and monetization,

Some of the data centres in India-

1. Ctrl S
2. NTT data centre
3. Adani data centre park
4. NPCI data centre
5. Google's data centre
6. ESDS data centre
7. Net4India



The National Digital Communications Policy 2018

The Telecom Regulatory Authority of India has recommended the formulation of the National Digital Communications Policy 2018. The objective of a national policy on digital communications is to prepare the country and its citizens for the future. It envisages establishing India as a global hub for cloud computing, content hosting and delivery, and data communication systems and services.

The National Communications Policy aims to accomplish the following Strategic Objectives by 2022:

1. Provisioning of Broadband for All
2. Creating 4 Million additional jobs in the Digital Communications sector
3. Enhancing the contribution of the Digital Communications sector to 8% of India's GDP from ~ 6% in 2017
4. Propelling India to the Top 50 Nations in the ICT Development Index of ITU from 134 in 2017
5. Enhancing India's contribution to Global Value Chains
6. Ensuring Digital Sovereignty

Data Empowerment and Protection Architecture (DEPA)

In August 2020, NITI Aayog released a discussion paper on Data Empowerment and Protection Architecture (DEPA). The main reason behind it is to provide individuals with the practical means to access, share, and use datasets containing their personal information in an accessible

and easily understandable manner. This includes purchase data, traffic data, telecommunications data, medical records, financial information, and data derived from various online services.

Digital Payment Systems

Digital Payment system is a process of making payment via digital or online modes. Here no physical exchange of money involved. It is also known as cashless transactions. Now all over across the world, we can make payment with the use of online or digital payment system. It makes the business transactions easiest one. We can make the payment at any place of the world. With digital payment, we can send and receive funds from anywhere in the world at the click of a button.

From barter system to Unified Payments Interface (UPI), payment systems in India have come a long way. The electronic payment system is considered as the backbone of e-commerce. This is a part of digital economy, where the currencies are exchanged digitally. When we make payment via digital modes, either from digital platforms or on physical premises, it qualifies as a digital payment. The terms "money" and "currency" are used interchangeably.

User of Internet and other social media platforms-

- Current population of India-138 crores (2020)
- Over 290 million Facebook users in India
- There were 65 090 000 Linkedin users in India in January 2020, which accounted for 4.6% of its entire population. And 180 million users in the United States, as of October 2021

Defining the terms

Meaning of virtual currency-It is a currency available in electronic form. As per Indian Revenue service, Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value.

Digital currency- Digital currency is a digital format of fiat money.

Crypto currency- cryptocurrencies are built on the blockchain. Cryptocurrencies are not under the control of any single entity.

Origin of Internet

The concept of internet was brought up by USA in 1950. Internet was started in India by VSNL LIMITED with an average speed of 9.6 Kbit/s in 1995. The speed later increased to 33.4kbit/s, with 14 lakh Indian users.

History of payment system

- **Barter system**- Method of exchange
  - exchange of goods and services without the use of money.
  - Introduced by Mesopotamia tribes, bartering was adopted by Phoenicians
  - Started in 6000 BC.
  - Firstly, farmer used these techniques to exchange wheat and other goods in exchange of of shoes from a shoemaker
- **Money system- Coins-**In 600 B.C., Lydia's King Alyattes imprinted the first official currency. These coins were made from electrum, a mixture of silver and gold that occurs naturally, and the coins were stamped with pictures that acted as denominations.
  - The first Indian coins were imprinted in the 6th Century BC **by the Mahajanapadas** (republic kingdoms) of ancient India. It was marked as a punch which was called as called Puranas, Karshapanas or Pana. It was made up of silver and bear symbols like-

  - **Transition to paper money-** In 770 B.C. it was the Chinese who devised the system of paper money for the first time.

Ancient India Coinage

- Punch Marked Coins
- Dynastic Coins- Indo-Greeks, the Saka-Pahlavas and the Kushans. 2nd century BC and 2nd century AD, Kushan coins
- Satavahana- Andhras (270 BC to 30 BC), silver coins of the Satavahanas carried portraits and bilingual legends,
- Western Kshatrapa- 1stand 4th Century AD- copper coins are the 'bull and hill' and the 'elephant and hill' types.
- Gupta coinage (4th-6th centuries AD)
- Post-Gupta coinage (6th-12th centuries AD)
- South Indian Coinage- symbols-dynastic crests such as the boar (Chalukya), bull (Pallava), tiger (Chola), fish (Pandya and Alupas), bow and arrow (Cheras) and lion (Hoysala)

Before Independence

- Foreign currency came to India when East India Company was started in India

After Independence

- The "Anna Series" was introduced on 15 August 1950. This was the first coinage of the Republic of India. The King's image was replaced by Ashoka's Lion Capital.
- These included 1/2-rupee, 1/4 rupee, 2 anna, 1 anna, 1/2 anna & 1 pice coins. one rupee was divided into 16 annas or 64 pice, with each anna equal to 4 pice.
- In 1957, India shifted to the decimal system- New Paisa. "naya" was dropped in 1964 and a new denomination, the 3 paisa, was introduced into circulation. A 20 paisa coin was minted in 1968
- In 2005, the 10-rupee coin was minted for the first time.
- On 30 June 2011, all coins in denominations of 25 paisa and below were officially demonetised.
- Present existing coins- One Rupee, Two Rupees, Five Rupees, Ten Rupees and Twenty Rupees.

Paper money-

- The first paper currency note, i.e., the 10 rupees' note was introduced by the Government of India in the year 1861.
- British India Issues commence with the Paper Currency Act of 1861 which gave the Government the monopoly of note issue in India
- The Reserve Bank of India was formally inaugurated on April 1, 1935 with its Central Office at Calcutta.
- First Five Rupee note was issued bearing the portrait of George VI in 1938.
- The George VI series continued till 1947 and thereafter as a frozen series till 1950 when post-independence notes were issued.

Banking cards

- Debit cards were introduced in 1966
- Credit card was introduced by the Central bank of India in 1980 in association with Visa and Master Card.
- Smart payment cards were introduced to the banking sector in 1979, and came into wider use in the mid-1980s.
- In 2004, the Payment Card Industry Security Standards Council was created to make sure that businesses comply with security requirements. This organization develops and implements security standards for account data protection.

Electronic Payments/ Mobile Payments

- It was started in 21st Century
- Mobile payments and virtual currency.
- India's first-ever payment aggregator "BILLDESK" launched its operations in India, in 2000.
- Mobile banking was started in 2007
- Bitcoin, released in 2009 by the pseudonymous Satoshi Nakamoto

Various types and methods of digital payments-

1. Banking Cards
2. Unstructured Supplementary Service Data (USSD)-
3. Aadhaar Enabled Payment System (AEPS)-
4. Unified Payments Interface (UPI)
5. Mobile Wallets
6. Bank Prepaid Cards
7. Point of Sale (PoS) Terminals
8. Internet Banking
9. Mobile Banking
10. Micro ATMs

1. **Banking cards**- It means the It includes-
    a) Debit card,
    b) credit card,
    c) prepaid – offers and
    d) electronic card

a) Debit card- It is the card which is used to deduct amount or to make payment from the customer's account. Money is taken out by this card which is already deposited in the account.

Types of debit card-

- Visa Debit Card
- Visa Electron Debit Card
- Mastercard Debit Card
- Maestro Debit Card
- RuPay Debit Card- The National Payments Corporation of India (NPCI)

b) Credit card- It is card which allows the user to make payment or withdraw amount by borrowings from the bank up to a certain limit.

c) **Prepaid offers-** It is not linked with the bank accounts. It is the card in which money is loaded to the card. That amount can be invested by the used for various purposes within the time limit.

d) **Electronic card-**It is mainly used for ecommerce transactions. It is also known as virtual card. This card can be used for limited time. Upto its validity. Various banks issue such types of cards like SBI.

2. **Aadhaar Enabled Payment System**-

- This system is developed by NPCI i.e. National Payments Corporation of India.
- to carry out financial transactions on a Micro-ATM by furnishing just their Aadhaar number and verifying it with the help of their fingerprint/ scan.
- Service Available from no. of operators: 118 banks
- Banking Services Offered by AePS
    - Cash Deposit
    - Cash Withdrawal
    - Balance Enquiry
    - Mini Statement
    - Aadhaar to Aadhaar Fund Transfer
    - Authentication
    - BHIM Aadhaar Pay

3. Unified Payments Interface (UPI)

- money will be directly debited from the customer's bank account.
- "Peer to Peer"
- immediate money transfer
- 2 Factor Authentication
- QR Code

UPI Payment App

1. PhonePe-
2. Paytm
3. BHIM app
4. MobiKwik
5. Google Tez
6. Uber
7. Chillr
8. Paytm Payments Bank
9. SBI Pay
10. iMobile
11. Axis Pay
12. BOB UPI

5. Mobile Wallets

   It is type of virtual or digital wallet. It stores various information such as debit and credit card numbers. It allows the user to make electronic transactions such as purchase of goods, electricity payment, recharge of mobile phones etc. An individual's account is required to be linked to the digital wallet to load money in it.

   Mobile wallet apps-

   1. Paytm
   2. Freecharge
   3. Google Pay
   4. Apple Pay
   5. Amazon Pay
   6. Mobikwik
   7. mRuppee
   8. Airtel Money
   9. Jio Money
   10. SBI Buddy

11. itz Cash
12. Citrus Pay,
13. Vodafone M-Pesa
14. Axis Bank Lime
15. ICICI Pockets
16. SpeedPay

Services Offered:

- Balance Enquiry
- Passbook/ Transaction history
- Add money
    - Bank A/c
    - All Cards
    - Cash-In
- Accept Money
- Pay money
    - Another wallet (mobile no.) with same provider
    - Pay merchant
    - Bar Code reader
- Manage Profile
- Notifications

5. Bank Prepaid cards

List of banks permitted by RBI to issue pre-paid cards in India as on April 05, 2021

1 Airtel Payments Bank Limited

2 American Express Banking Corporation

3 A. P. Mahesh Co-operative Urban Bank Limited

4 Au Small Finance Bank Limited

5 Axis Bank Limited 6 Bandhan Bank Limited

7 Bank of Baroda

8 Bank of India

9 Bank of Maharashtra

10 Barclays Bank PLC

11 Canara Bank

12 Central Bank of India

13 Citi Bank N.A.

14 City Union Bank Limited

15 DBS Bank India Limited

16 DCB Bank Limited

17 Equitas Small Finance Bank Limited

18 ESAF Small Finance Bank Limited 1

9 Fino Payments Bank Limited

20 First Rand Bank

21 HDFC Bank Limited

22 ICICI Bank Limited

23 IDBI Bank Limited

24 IDFC FIRST Bank Limited

25 Indian Bank

26 Indian Overseas Bank

27 IndusInd Bank Limited

28 Jana Small Finance Bank Limited

29 Jio Payments Bank Limited

30 Karnataka Bank Limited

31 Karur Vysya Bank Limited

32 Kerala Gramin Bank

33 Kotak Mahindra Bank Limited

34 Lakshmi Vilas Bank Limited

35 NSDL Payments Bank Limited

36 Paytm Payments Bank Limited

37 Pragathi Krishna Gramin Bank

38 Punjab National Bank

39 Punjab & Sind Bank

40 SBM BANK (INDIA) LTD.

41 South Indian Bank Limited

42 Standard Chartered Bank

43 State Bank of India

44 Tamilnadu Mercantile Bank Limited

45 The Ahmedabad Mercantile Co-operative Bank Limited

46 The Catholic Syrian Bank Limited

47 The Dhanlaxmi Bank Limited

48 The Federal Bank Limited

49 The Gujarat State Co-operative Bank Limited

50 The New India Co-operative Bank Limited

51 The Rajasthan State Co-operative Bank Ltd.

52 TJSB Sahakari Bank Limited

53 RBL Bank Limited

54 The Saraswat Co-operative Bank Limited

55 UCO Bank

56 Union Bank of India

57 Yes Bank Limited

6. **Point of Sale (PoS) Terminals**

   It means the payment made by the customer at the time of purchasing at the counter via electronic means. It involves processing of card payments at retail locations.

7. **Internet Banking-** is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions

through the financial institution's website. It is also known as online banking or e-banking.

8. **Mobile Banking**- It can be done by installing the app of the financial institution in mobile phones. It involves the act of making financial transactions on a mobile device (cell phone, tablet, etc.).
9. **Micro ATMs**-It is also known as mini-ATM. are portable devices that allow banking transactions including cash deposit, withdrawal and fund transfer using debit or RuPay cards. It is the used by the business merchants to provide banking services to its customer. This machine contains facilities like card swiping and fingerprint scanner.

Establishment of institutions

- Institute for Development and Research in Banking Technology (IDRBT)- https://idrbt.ac.in/- It was established in March 1996 as an Autonomous Centre for Development and Research in Banking Technology.
- National Payments Corporation of India (NPCI)
- Clearing Corporation of India Limited (CCIL)

National Payments Corporation of India-NPCI- https://www.npci.org.in/

It is an initiative taken by the Reserve Bank of India (RBI) and Indian Banks' Association (IBA) to set up an organization to operate payment and settlement system in India. This organization is established under the provisions of the Payment and Settlement Systems Act, 2007. It is Non-Profit organization established under Section 8 of the Companies Act 2013.

Payment system developed by NPCI

- RuPay
- Immediate Payment Service (IMPS)
- National Automated Clearing House (NACH)

- Aadhaar Payment Bridge System (ABPS)
- Aadhaar enabled Payment System (AePS)
- National Financial Switch (NFS)
- Unified Payments Interface (UPI)
- Bharat Bill Payment System

Payment gateways in India

i. Citrus Pay Payment Gateway- https://consumers.citruspay.com/

ii. CCAvenue Payment Gateway- https://www.ccavenue.com/

iii. PayUBiz India Payment Gateway- https://www.payubiz.in/

iv. Direcpay Payment Gateway- https://www.direcpay.com/

v. Zaakpay Payment Gateway- https://zaakpay.com/

vi. Instamojo Payment Gateway- https://www.instamojo.com/

vii. Bill Desk- https://www.billdesk.com/

viii. Atom Paynetz Payment Gateway- https://www.atomtech.in/

ix. PayUMoney- https://payu.in/

x. ePaisa- https://www.epaisa.com/

xi. airpay- https://sanctum.airpay.co.in/

xii. JusPay- https://juspay.in/

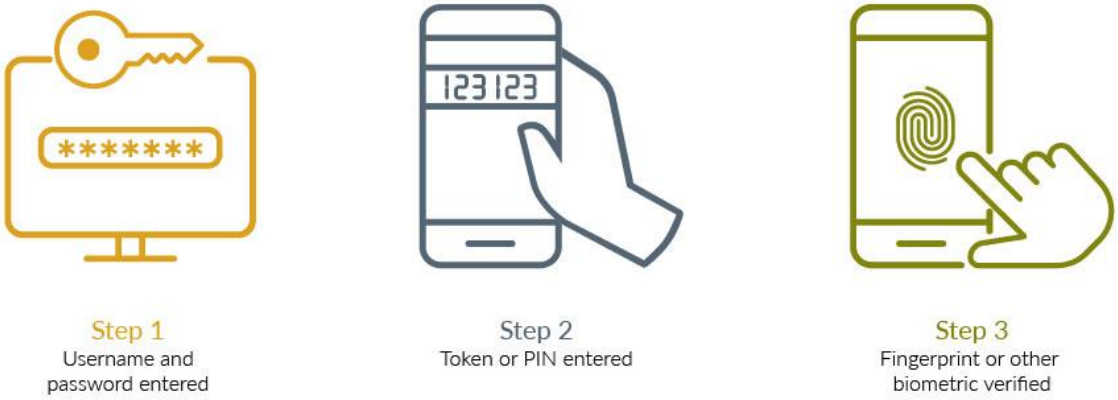
xiii. Transecute- https://www.transecute.com/

Authentication for digital payment

1. Multifactor authentication-It includes-

- Password-based authentication,
- 3D secure,

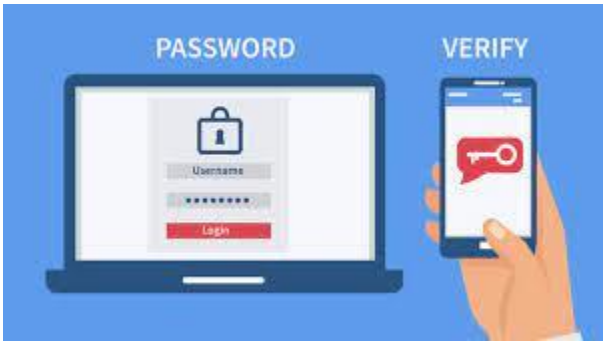
- Card Verification Value (CVV),
- address Verification Systems (AVS),
- Age Verification,
- time-based one-time password (TOTP) method,



2. Two-factor authentication-two-step verification or dual-factor authentication.

Example-withdrawing of money from an ATM; It requires to the user only the correct combination of a bank card and a PIN in order to carry out the transaction.

Like Google- 2 step verification, Amazon Two-Step Verification, Apple Two-Factor Authentication



Who acts as regulator and supervisor of payments and settlement system in country?

Payment and settlement systems in India are used for financial transactions. They are covered by the Payment and Settlement Systems Act, 2007 legislated in December 2007 and regulated by the Reserve Bank of India and the Board for Regulation and Supervision of Payment and Settlement Systems.

Payment and settlement systems

In India, the payment and settlement systems are regulated by the Payment and Settlement Systems Act, 2007 which was legislated in December 2007. Also, the Payment and Settlement System Regulations, 2008 framed thereunder came into effect from August 12, 2008. The Reserve Bank of India is the regulatory authority who operates payment and settlement system in India.

The Board for Regulation and Supervision of Payment and Settlement Systems (BPSS), a sub-committee of the Central Board of the Reserve Bank of India is the highest policy making body on payment systems in the country.

Who heads the board for payment and settlement system?

The Board for Payment and Settlement Systems is chaired by the Governor of RBI and its members are all the four Deputy Governors and two Non- Official Directors of the Central Board.

The Payment and settlement System Act, 2007-Legislated on 20th December, 2007
This act provides for the regulation and supervision of payment systems in India. It was legislated to designate RBI as the authority for the payment and settlement system in India. It contains 8 Chapters, 38 Sections.

Various definitions under the Payment and settlement System Act, 2007
"payment instruction" means any instrument, authorisation or order in any form, including electronic means, to effect a payment,

(i) by a person to a system participant; or

(ii) by a system participant to another system participant

“payment obligation” means an indebtedness that is owned by one system participant to another system participant as a result of clearing or settlement of one or more payment instructions relating to funds, securities or foreign exchange or derivatives or other transactions;

“payment system” means a system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange;

“settlement” means settlement of payment instructions and includes the settlement of securities, foreign exchange or derivatives or other transactions which involve payment obligations.

“system participant” means a bank or any other person participating in a payment system and includes the system provider

“system provider” means a person who operates an authorised payment system

Various Powers of RBI-

1. Power to determine standards
2. Power to call for returns, documents or other information
3. Access to information
4. Power to enter any premise where a payment system is being operated and to inspect any equipment, including any computer system or other documents situated at such premises.
5. Power to carry out audit and inspection
6. Power to issue directions
7. Power to give general directions

RBI directions or framework for digital payment-

- RBI Framework for Facilitating Small Value Digital Payments in Offline Mode, January 03, 2022
- The Reserve Bank of India (Digital Payment Security Controls) directions, 2021, February 18, 2021
- RBI Guidelines for the issue of Smart / Debit Cards by banks, November 12,1999

Committee Report on Deepening of Digital Payments

- Constituted by RBI
- High Level Committee- Chairman- **Nandan Nilekani**
- Submitted report on - May 17, 2019

The Committee in its report included the following:

(i) reviewing the existing status of digital payments in India,

(ii) identifying gaps and recommending measures to bridge them,

(iii) assessing the current levels of digital payments in financial inclusion and

(iv) suggesting a medium-term strategy for deepening of digital payments.

The Unique Identification Authority of India (UIDAI)- https://uidai.gov.in/

It is a government agency established under the provisions of the **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act 2016")** on 12 July 2016 by the Government of India, under the Ministry of Electronics and Information Technology (MeitY).

UIDAI is responsible for Aadhaar enrolment and authentication, including operation and management of all stages of Aadhaar life cycle, developing the policy, procedure, and system for issuing Aadhaar numbers to individuals and perform authentication and **the security** of identity information and authentication records of individuals.

Total Aadhaar issued-131.68 crore Aadhaar numbers to the residents of India.

What services Chartered Accountants can render in Digital economy?

1. Digital Transformation Consultancy services
2. Startup ecosystem
3. Create a website
4. Fintech services
5. Set up your own blog or contribute blog posts on various CA platforms
6. Conferences and Public Speaking Opportunities in virtual mode
7. Become An Affiliate of Network of Chartered Accountants
8. Create Profiles on social media
9. Join Groups on Various Social Media Platforms
10. DSC Agency
11. Digital Marketing Coaching
12. Big data create new opportunities for businesses and consumers, and new challenges for security and privacy
13. Big data analytics
14. Assistance in social media
15. Data Protection laws
16. Audit of documents, maintained in electronic form
17. Awareness about privacy and data protection frameworks and strengthen their enforcement
18. Solutions to address digital security issues
19. Governance approach that supports co-ordination, articulating a strategic vision, assessing key digital trends and policies
20. Ensure technical enablers are in place, such as Internet exchange points, efficient allocation of spectrum and new generation Internet protocol addresses. Reduce administrative barriers to investment, such as burdensome licensing requirements and complex rights of way.
21. empower everyone with a mix of skills to thrive and trust in a digital world.
22. review education and training systems to better exploit the possibilities of digital learning

23. promote investment in digital technologies and intangible assets (e.g., patents, software)
24. Data Centre Audit

"Ability is what we are capable of doing. Motivation determines what we do. Attitude determines how well we do it."

Websites for references

https://data.worldbank.org/

https://www.weforum.org/

http://cashlessindia.gov.in/

https://uidai.gov.in/

https://www.npci.org.in/

https://dot.gov.in/