
# National e-Governance Conference

## BACKGROUND PAPERS

## CONTENTS

# Chapter 1

## Digital Governance Across Whole-of-the-Government

*Author - Dr. Ramanand N. Shukla*

*Director, Quality Council of India*

**What is Digital Governance?**

Digital governance refers to carrying out governance process in a digital way to deliver digital services and is also known as electronic governance (e-governance), transformational governance, and connected governance. It entails application of information and communications technology by government agencies to their functioning for making simple, moral, accountable, responsive and transparent (SMART) governance a reality.

Digital governance is not about translating processes but is about transforming them to bring transparency, accountability and efficiency in the government agencies and their services. Digital governance or e-governance is based essentially on four pillars.

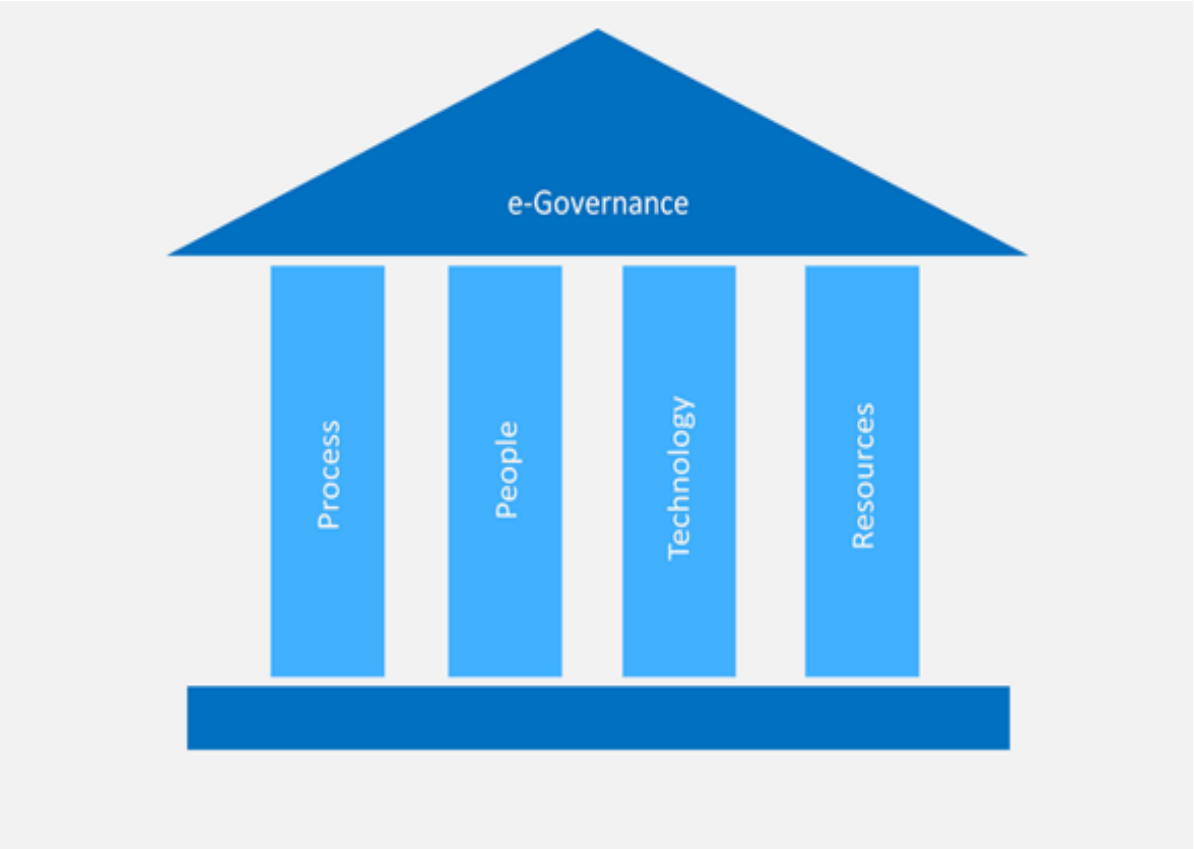



Fig. 1 Four Pillars of Digital Governance

The key considerations of the four pillars in digital governance are:

| | |
|---|---|
| **Pillar 1: Process**<br><br>- Simplicity<br>- Efficiency<br>- Citizen-centricity<br>- Sustainability<br>- Cost-effectiveness | **Pillar 2: People**<br><br>- Vision<br>- Leadership<br>- Commitment<br>- Competency<br>- Change |
| **Pillar 3: Technology**<br><br>- Architecture<br>- Open standards<br>- Reliability<br>- Scalability<br>- Security | **Pillar 4: Resources**<br><br>- Holistic<br>- Efficient<br>- Service-oriented<br>- Sustained<br>- Adequate<br>- |

**Digital Governance in India: Empowering citizens, Improving efficiency**

Digital Governance has led to an incredible transformation in the way governments serve citizens and accomplish critical missions. Governance in India has also seen a remarkable transformation as the government has been proactively adopting technology for economic revival and inclusive growth. Digital governance in India is focused on empowering citizens, driving industrial development, enhanced co-operation between Center and states, transparent and efficient delivery of government services, ease of doing business, job creation and development of infrastructure which are all enablers for economic revival and inclusive growth.

Recently, the world witnessed how the Indian government leveraged technology for empowering citizens and their well-being through CoWIN platform which was also made available to the world to help them in their fight against Covid-19 pandemic. This digital approach not only made it easy for the citizens to plan and get their vaccinations but also helped in tracking the usage of vaccination and minimizing the wastage.

Implementation of the initiatives under the digital governance has enabled huge savings in costs through sharing of core and support infrastructure, enabling interoperability through standards, and presenting a seamless view of Government to citizens.

As a part of digital governance programme, the government has launched several flagship initiatives such as Aadhar, Pradhan Mantri Jan Dhan Yojana (PMJDY), Direct Benefit Transfer (DBT), PM's Bima Yojana, Pradhan Mantri Jan Arogya Yojana (PMJAY) smart cities, etc. that have helped to reach out to the citizens at the last mile with a focus on inclusive growth.

Many of these digital governance programmes have been path breaking and lauded globally. For instance, the Aadhaar programme.

Aadhaar is perhaps the world's largest biometric identification programme in the world with about 99 percent of adult Indians holding an Aadhaar ID that links to around 84 government services, including the country's food distribution system, the world's biggest welfare programme. The Aadhar system has been even commended by Paul Romer, Chief Economist at the World Bank. He said, "The system in India is the most sophisticated that I've seen," "It's the basis for all kinds of connections that involve things like financial transactions. It could be good for the world if this became widely adopted."

According to the DBT Portal, DBT and other governance reforms have led to removal of duplicate/ fake beneficiaries and plugging of leakages etc., as a result of which the government has been able to target the genuine and deserving beneficiaries and in the process, has cumulative estimated savings of Rs. 1.41 trillion till 2019.

Similarly, the Pradhan Mantri Jan Dhan Yojana (PMJDY) set a world record for most number of bank accounts opened under a financial inclusion programme in a week. PMJDY has also been one of the most far reaching initiatives towards Financial Inclusion not only in India but in the world. **It provides an avenue to the poor for bringing their savings into the formal financial system, an avenue to remit money to their families besides taking them out of the clutches of the usurious money lenders.**

Adoption of technology and a clear vision for digital governance across whole-of-the-government has helped the government to reach out to the masses and create significant impact across board.

However, this leap into digital governance in India was not overnight. It began with computerization of Government Departments and over the years, a large number of initiatives were undertaken by the Central Ministries and various State Governments to usher in an era of Digital governance, encapsulating the finer points of Governance, such as citizen centricity, service orientation and transparency. This encompassed implementation across the various arms of Government at National, State, and Local levels through several policy interventions and initiatives guided by common vision and strategy.

A glimpse of some of the other major initiatives as a part of the digital governance are mentioned below:

**DARPAN: It is an online tool that can be used to monitor and analyze the implementation of critical and high priority projects of the State. It facilitates presentation of real time data on Key Performance Indicators (KPIs) of selected schemes/projects to the senior functionaries of the State Government as well as district administration.**

**PRAGATI (Pro-Active Governance and Timely Implementation): It has been aimed at starting a culture of Pro-Active Governance and Timely Implementation. It is also a robust system for bringing e-transparency and e-accountability with real-time presence and exchange among the key stakeholders.**

**Common Services Centres 2.0 (CSC 2.0): It is being implemented to develop and provide support to the use of information technology in rural areas of the country.**

**e-Kranti: It aimed at the expansion of the internet, mobile phones, and computers to rural areas. The scheme includes the starting up of IT-based jobs in rural areas and also the linking of the internet to the remote villages of the country. There are 44 Mission Mode Projects under the e-Kranti program.**

**e-Courts:** Launched by the Department of Justice, Ministry of Law and Justice, this Mission Mode Project (MMP) aims at utilizing technology for improved provisioning of judicial services to citizens.

**e-District: Launched by the Department of Information Technology, it aims at delivery of high volume, citizen-centric services at the District level such as the issue of birth/death certificate, income and caste certificates, old age and widow pension, etc.**

**e-Panchayats: The government has launched the e-governance scheme known as e-panchayats to improve the quality of governance in Panchayati Raj Institutions.**

**MCA21:** Launched by the Ministry of Corporate Affairs with an aim to provide electronic services to the Companies registered under the Companies Act.

**e-Office: Launched by the Department of Administrative Reforms & Public Grievances with an aim to support Governance by ushering in more effective and transparent inter and Intra-Government processes.**

**DigiLocker: It serves as a platform to enable citizens to securely store and share their documents with service providers who can directly access them electronically.**

**e-Hospital-Online Registration Framework (ORF): It is an initiative to facilitate the patients to take online OPD appointments with government hospitals. This also covers patient care, laboratory services and medical record management.**

**All such initiatives are a step forward towards** creating a robust digital governance framework for making simple, moral, accountable, responsive and transparent (SMART) governance a reality.

**Way Forward**

Digital Governance is not just about online systems and infrastructure; it is ultimately about shaping the future of citizens by empowering them and promoting inclusive growth which can happen only by reaching out to citizens in the remotest of locations and make them achieve their aspirations. India's vast expanse and differences in demographics, pose a challenge to the people in remote areas in accessing various government schemes and benefits. Digital governance is an answer to overcome such challenges by empowering citizens and ensuring equitable & inclusive growth which could be seen through the successes of various digital government programmes.

However, to ensure success of its digital governance programmes, the government will have to proactively address the following key areas:

**Regulatory framework:** The government should focus on instituting a robust regulatory framework for seamless implementation and adoption of digital services. This would be very important for building trust among the public towards government services for quick adoption.

**Effective design and implementation:** An effective implementation depends on the quality of design and therefore, the digital governance programmes should be designed meticulously considering the need of the users. Given the highly developed IT capabilities within the country, private sector expertise can be leveraged for designing of such programmes and systems. Further,

focus should be on the right enablers for effective implementation i.e., robust planning, futuristic, agile and scalable implementation practices.

**Digital divide:** Among various other challenges one of the key challenges is the digital divide. Due to economic poverty, a large number of people are unable to afford digital devices. The government will have to focus on ensuring affordable devices and digital services for all.

**Security and privacy:** With digitalization becoming an integral part of the lives of citizens, security and privacy issues will require special attention and focus. Digital governance without assurance of security and privacy to the citizens in today's times of increasing cybercrimes, would not only risk everyone in the system but may lead to serious consequences.

# Chapter 2

## Digital Economy: Strengthening Start-up Ecosystem & Employment Generation

Author - Dr Sachchidanand Shukla* & Sarbartho Mukherjee**(views personal)
[*Chief Economist, Mahindra Group & **Economist, M&M]

Over the last few years, the start-up ecosystem has witnessed robust growth in India. The Centre, in 2016, launched the 'Start-up India Initiative' to build a robust ecosystem for nurturing innovation in the country. Since then, the number of DPIIT-recognised start-ups has grown from 471 in 2016 to more than 81,000 today. With the rising diffusion of ICT, industrial policies have metamorphized from traditional factory-based production-based initiatives to a more innovation-based initiative aimed at accelerating the adoption and diffusion of technologies like 5G and AI. This transition was also accentuated by India's long-term investments in STEM education and public funding of the research. Key focus areas of government have been R&D grants, tax benefits for start-ups, business incubators, and facilities for university-based spin-offs.

### Is the digital economy aiding start-up ecosystems, or is it vice versa?

The interlinkages between the start-up ecosystem and the digital economy are so intricate that growth in one of these sectors is bound to pull the other. The digital economy is created by all the economic activities that result from higher online/digital connections among people, businesses, and machines. Hyperconnectivity forms the digital economy's backbone, resulting in higher interconnectedness due to the internet and IoTs. Thanks to investments made in the ICT infrastructures over the past few decades by both public as well as private players, India currently has a solid interconnected economy which is expected to grow by leaps and bounds in the coming years. This strong foundation of the domestic ICT infrastructure has helped to create a robust digital economy which in turn has aided start-up ecosystems in the following ways:

- **Data valuation and information economics:** A highly interconnected world with a strong and growing interlinkage between consumers, businesses and machines has resulted in data generation. The data is often used and processed by start-ups, resulting in value creation. Since information or big data is the new oil of the digital world, start-ups are actively looking for ways to extract, refine and process it to generate insights. Data has become so valuable that countries are looking at in-house data centres for storing data, with strong growth in the number of data centres.
- **Increase in ease of doing business to lower cost of doing business:** An interconnected world has not only increased the ease of doing business but also lowered the cost of doing business. Due to higher interconnectedness, digital technologies can generate clear advantages for businesses, including cost savings, operational efficiency, IT resilience and scalability, easier access to new markets, and market effectiveness. ICT enhance the productivity of both labours as well as capital. Even non-technology start-ups and small entrepreneurs can access markets via online market platforms created by the digital economy.
- **Geography is no longer a barrier:** The enhancement in the digital economy has helped in deepening the distribution of start-up environments. Apart from the top metro cities of India, the start-up ecosystem is fast growing in the Tier II cities of India, like Jaipur, Lucknow, and Indore. The deagglomeration of the start-up ecosystem has been aided by growing internet penetration, making it easier for scaling up ventures. Additionally, remote working has helped to access talent for the ventures working from these cities.

While the digital ecosystem adds impetus to the start-up ecosystem, the start-up ecosystem helps enhance the digital economy by working as a hub of innovation. A start-up environment focusing on Information Technology and ICT creates a hub for innovation that fuels a digital economy's enhancement. One of the key examples of a start-up ecosystem helping the digital economy is the famous Silicon Valley of the US, one of the distinguished sources of innovation that dominates the tech world around the globe.

### Policy aids in strengthening the digital framework

For harnessing digital technology & fostering innovation, the Ministry of Electronics & IT (MeitY) has been focussing further on deepening the Digital India Programme 2.0. A few months back Prime Minister launched the 'Digital India Genesis' AND 'Indiastack.global' program along with the list of the first cohort of 30 Institutions to be supported under the 'Chips to Start-up Programme'. MeitY, through these schemes, looks to support more than 2,000 start-ups with a yearly budgetary outlay of INR 1 bn. With its slew of initiatives, especially tailor-made for Tier II & Tier III cities and semi-urban areas, MeitY is paving the way for massive penetration of start-up ecosystems in these areas.

While policy actions are aimed at the deagglomeration of the start-up ecosystem, it brings in their own set of challenges in terms of creating safeguards for data protection, privacy, payment safety and consumer protection. New sectors like online gaming, non-bank digital lending, IoT and AI need newer regulations. The government taking cues from the financial industry, needs to follow a co-regulation model to tackle the challenges posed by the new industry. Various agencies and industry bodies comprising a statutory oversight body, industry-led self-governance norms and multi-level grievance redressal mechanisms must work in tandem to solve the issues arising. Given these industries' complex nature, co-regulation and self-governing norms will be best for sector-specific needs. Examples of these co-regulating models exist in the western world, such as the Entertainment Software Rating Board of the Entertainment Software Association in the US, which assigns age and content ratings to consumer video games. Better regulations will not only protect the industry from unintended consequences but will also instil confidence among the consumers of the digital economy.

### High interest rates along with a risk-off environment to pose challenges in the near term

The world is currently witnessing a significant pullback in venture capital (VC) funding, and India is no exception. Rapidly rising interest rates in the advanced economies such as the US and EU have raised risks of a recession in major global economies. Geopolitical uncertainties have resulted in a sharp rise in the risk-off sentiments globally. As a result, investors are looking for safe-haven investments as priorities have shifted towards wealth preservation. Aggressive tightening accompanied by quantitative tightening (QT) by the leading global central banks will keep the cost of money elevated for longer and weigh on firms' valuation. New-age firms, which rely on prospects of strong future cash flows, have been the worst hit as a higher interest rate environment resulted in a sharp discounting, reducing their valuations significantly.

Recent data suggests a funding crunch for Indian start-ups as VC funding in India dropped to its lowest point since Q1 2020. VC-backed companies received only ~ USD 2.9 bn in the June-September quarter of this year, a drop of ~ 66% QoQ and ~81% YoY. A sharp drop in valuation and funding crunch has resulted in higher consolidation among start-ups. There were 203 M&A among Indian start-ups in CY2022 till the September quarter, which is ~60% above the average annual M&A in the pre-pandemic period of 2017-2019. However, this blip is expected to be short-lived as growth potential remains robust in the Indian economy.

### But don't forget the growth and demographic advantage – From Job seekers to Job makers

India has emerged as a global powerhouse and the economy is expected to cross USD 5 tn in the next few years. India has undergone a phenomenon of low employment intensity with respect to GDP growth as even higher rates of growth in GDP didn't match well with the growth rate in jobs in the last couple of decades. India's labour force participation stands at ~40%, implying that less than half of the working-age people are open to work. India needs to create more jobs, especially in the manufacturing sector. Added to that, the recent evidence of capital deepening further worsens the situation. Going ahead, progress in science and technology along with the advancement in robotics and AI would further accentuate capital deepening and job growth. Since the 1980s, real capital employed per unit worker has almost tripled for the whole economy, with the fastest growth in mining, manufacturing, and services. Even though we still have huge labour abundance, producers still continue to complement capital stock with labour as it improves productivity and solves the problem of shortage of a skilled labour force. It is expected that capital deepening will further accelerate after the pandemic as digitization increases in society.

India has entered "Amrut Kaal" with the potential of reaping the demographic dividend over the next thirty years. Against this backdrop, job creation remains the key objective of the government. Apart from the traditional manufacturing and services sectors, the recent rise of the start-up ecosystem is going to be a key

engine of job creation in the medium to longer term. As per the government's own estimates, DPIIT-recognized start-ups registered in India over the past six years generated about ~8 lakh jobs over this period. India currently has more than 100 unicorns. As new start-ups mature and expands, the number of unicorns is expected to grow further. A closer look at the labour market of the western world reveals that young firms play an important role in job creation. On average, across OECD countries, young firms account for about 20% of employment but create almost half of new jobs. Confederation of Indian Industry (CII) has estimated that India's economy can grow from the current USD 3.3 tn to USD 9 tn and USD 40 tn by 2030 and 2047, respectively, if its working-age population, which is expected to increase by over 100 million people in the next eight years, is productively employed.

The government's focus on start-ups not only aims to solve the problem of job seekers but encourages an environment of entrepreneurship with job creators. Policy measures like Innovation in Mobile App Development Ecosystem (I-MADE) and PM Mudra Yojana aim to promote the culture of entrepreneurship. Going ahead, the success of these policies will determine the extent to which the country can benefit from a demographic advantage, thereby avoiding a middle-income trap.

**References**


- DPIIT recognised Start-ups and Policy: https://dpiit.gov.in/sites/default/files/ls244.pdf
- CII Estimates: https://indbiz.gov.in/india-can-become-us40-trillion-economy-by-2047-if-the-working-population-is-employed-cii/
- India's start-up M&A: https://inc42.com/features/2022-funding-winter-indian-startup-mas/
- VC funding to Start-ups: https://news.crunchbase.com/sections/data/
- Job creation by new age firms in OECD: https://www.oecd.org/industry/dynemp.htm
- Developing Entrepreneurship in Digital Economy: The Ecosystem Strategy for Startups Growth: https://www.researchgate.net/publication/332778308_Developing_Entrepreneurship_in_Digital_Economy_The_Ecosystem_Strategy_for_Startups_Growth/fulltext/5cc908004585156cd7bdd699/Developing-Entrepreneurship-in-Digital-Economy-The-Ecosystem-Strategy-for-Startups-Growth.pdf

# Chapter 3

## Modern Cyber Laws to Promote National Growth and to Secure Citizen's Rights – An Analysis of Indian Information Technology Act, 2000 and Need to Revamp the Present Laws to Meet the Challenges in the Cyber

Authors - Bhavna Sharma, Assistant Legal Manager, Cyber Law Division, Ministry of Electronics & Information Technology & Dr. Gaurav Gupta, Scientist- E, Cyber Law Division, Ministry of Electronics & Information Technology

**Abstract** – India is going to be upcoming nerve centre for Information Technology but simultaneously it also growing as a hub for cyber offences and data breeches and ill usage of technology by the individuals, public and private sector companies, and other governmental and non-governmental organisations. In such situation, it becomes significant to protect the digital rights of the internet users, fix accountability of the intermediaries involved in deceptive practices, oblige the intermediaries with certain best practices and due diligence, imposing higher penalties, and taking other measures to ensure user safety and wellbeing on the internet. For this, a modern cyberlaw is called for to combat all the existing and future predicted challenges in the coming times. In this article, the authors have talked about the background of the present cyber law in India, laid down the foundational pillars to be considered while making a modern cyber law and provided recommendations and challenges on how to address the prevailing issues to make a better cyber world.

### Background of The Technology Law in India

The Information Technology Act ("IT Act") was notified into law on the 17th October 2000, aligning India's legal framework with the model law on e-commerce and electronic signature proposed by the United Nations Commission on International Trade Law ("**UNCITRAL**"). Through its provisions, it gave statutory recognition to electronic records and digital signatures, defined cyber-crimes, prescribed penalties, while also appointing Adjudicating Officers and establishing an Appellate Tribunal to settle disputes under the statute. It became the de-facto framework for digital governance in India.

The first decade of the 21st century saw an increase in e-commerce activities in India and new forms of online transactions and platforms emerged. However, such transformation was accompanied by a steep rise in instances of computer misuse. This prompted a review of the IT Act. Subsequently, in 2008, the IT Act was amended, bringing in provisions relating to data protection, intermediary liability and exemption, and gave authorities the power to intercept, monitor, decrypt, and block information. The 2008 amendments also expanded the list of cyber offences— such as the introduction of the offence of child pornography, dissemination of obscene content, identity theft, cyber terrorism.

The IT Act was envisioned as a legislation to account for the emerging information technology ecosystem and the paradigm shift in online transactions and interactions. However, the speed of rapid developments in the information technology sector and increasing digitization has outpaced corresponding updation in lar worldwide. Large scale adoption of the internet and use of data has transformed how businesses operate and interact with consumers. New forms of online businesses have emerged that have changed the way we consume

entertainment, news, and information. There has also been an increase in new forms of harmful online activity and offences, especially impacting vulnerable groups, such as revenge pornography, cyber frauds, misinformation and disinformation. There has been a steep rise in the number of cyber-attacks and security incidents coupled with a drastic change in their scale and impact. The National Cyber Security Policy, 2013 is also being revised to keep abreast with these developments. Furthermore, jurisprudence around intermediary liability and protection of data and privacy has also evolved in the past decade. This requires urgent legislative and policy intervention in a manner that equitably addresses the concerns of all stakeholders.

Aside from the rapidly evolving digital landscape, the importance of the economic impact of the information technology sector in India has also precipitated the need to review the IT Act and other related acts. The IT sector has the capability to increase the productivity of every other sector of the economy while making governance more efficient and responsive. Furthermore, Indian information technology companies need to increase their participation and contribution in technologies such as machine learning, artificial intelligence and the Internet of Things if India is to effectively compete with global technology leaders. Thus, the IT and digital sector in India needs to be buoyed by innovation-enabling legislation and a regulatory regime that allows India to be a 'third pole' in the global cyber domain. This will help achieve its targets under the '*Digital India'* and *'Atmanirbhar Bharat'* initiatives which have become even more imperative in light of the Covid-19 pandemic.

Control over vast swathes of cyberspace lies in the hands of a few large entities which occupy a dominant position in the market. They have emerged as highly profitable advertising businesses that exert tremendous monopoly in the market and end up shaping market rules. These large entities adopt practices that further vertical integration and promote self-p referencing (they tend to promote their products and services more than those of their rivals on their own platforms). Adequately addressing antitrust challenges and such large platforms is one of the biggest regulatory obstacles facing the government. The platformization of the economy places an onus on the government and administrators to provide a level playing field. This would also help increase consumer choice and safeguard user rights. However, while attempting to administer and regulate such entities it must keep in mind that the obligations sought to be imposed do not apply too broadly as this will place a compliance burden that can be easily met by these large entities but not by their smaller competitors. Therefore, an enabling framework becomes critical to ensure that such large entities do not abuse their market power, obfuscate compliance, and are made subject to the jurisdiction of Indian courts. This requires sophisticated legislative instruments, policy interventions and a return to first principles.

Revisiting India's IT Act presents a unique opportunity to address India's distinct digital challenges while also removing ambiguities around technology in law, re-examining the role of actors in cyber-space, ensuring the safety and well-being of Indian users and creating a stable and effective regulatory environment. The time is ripe to bring in a legislation that accounts for the existing as well as emerging concerns in the information technology sector, through a targeted, streamlined, and comprehensive approach.

### Approach and Foundational Pillars for addressing the existing challenges in the cyberspace

The government sought to assess the adequacy of the existing cyber law against current and evolving needs of the sector and if necessary, replace it with a new, holistic and streamlined modern legislation. Such a legislation

shall adequately and appropriately address advancement in technologies, ensure a safe and open internet, enhance user safety and accountability of online platforms, and promote ease of doing business.

As emerging technologies drive new forms of business, service and delivery models leveraging artificial intelligence, machine learning, cloud and internet of things. The need of the hour is to rapidly create, modify, and enforce regulations. Effective governance of evolving information technology and digital developments would require open, agile and multi-stakeholder regulatory models. Therefore, modern cyber law must account for the interests of all stakeholders across the society, government and business. It should do so in an equitable, balanced and inclusive manner.

In formulating the modern cyber law, principles and outcomes-based approach to regulation must be adopted which provides a legislative framework with measurable impacts. Such an approach must focus on securing compliance with the rule of law as well as with principles such as user well-being, integrity, resilience, certainty, neutrality, accountability, transparency, market orientation, safety and security, efficiency and responsible technology design.

Following should be considered as the foundational pillar for addressing the identified action areas in the digital world -

i. ***User Well Being:*** Any regulatory framework for the digital domain must be built around users of the digital ecosystem as well as society at large. In this context, it is proposed to adopt a rights-based approach to regulation in a manner that helps build a foundation of trust amongst Indian users and digital actors while encouraging continuous growth across the digital economy. This may be achieved through modern cyberlaw by providing for a digital charter of user rights vis-à-vis digital actors that ensures a safe and trusted internet, online safety, protects privacy, and promotes transparency and accountability in the functioning of digital actors and in the design and deployment of new technologies.

ii. ***Accountability of Digital Actors****:* We must be cognizant of the innovations and developments in digital products, services and technologies and the accompanying complexities in the business models and operations. Therefore, it believes that modern cyberlaw should identify the different stakeholders and the products and services that need to be regulated. A holistic regulatory framework must be put in place that can carve out tailored obligations keeping in mind the nature, scale, and impact of such stakeholders. It is also recommended the regulation of emerging technologies, such as digital assistance products, Internet of Things, blockchain have become increasing popular, should be responsive and risk-based. A responsive approach would involve detecting undesirable or non-compliant behaviour, responding to such behaviour by developing appropriate legislative and regulatory tools and strategies, enforcing them and monitoring their success at the ground level and modifying them accordingly, whereas a risk-based approach would involve multi-stakeholder consultations and an engagement with data that goes beyond projected fears and growth narratives. A healthy and informative debate around the risks associated with new technology will help create a proportionate regulatory framework that balances innovation and protection effectively.

iii. ***Governance and Adjudication*****:** India lacks a responsive governance mechanism intended at protecting users and ensuring India's strategic priorities in the realm of cyberspace are consistently and comprehensively dealt with in a time-bound manner. Hence, in order to be able to respond to the fast-paced demands of the digital economy and to promote businesses to be conducted digitally, there is a need to ensure a unified, coordinated, speedy, efficient, and robust governance architecture**.** Therefore, it is believed that to ensure the effectiveness of India's governance, administrative as well as adjudicatory and dispute resolution framework for cyberspace, the modern cyberlaw must provide for a dedicated and specialised governance framework, including a regulator, inquiry agency and dispute resolution framework.

**iv.** ***Security of Cyberspace***: The increasing adoption of internet across all levels of the society and sectors makes cyberspace a vulnerable attack surface. Threats and risks to the cyberspace also continue to evolve every day, leading to new and emergent concerns about national security. We are also witnessing a multi-fold increase in the number and complexity of cyberattacks. Therefore, addressing such challenges is essential to India's national security, cyber resilience and to ensure and preserve India's digital sovereignty. Additionally, cyberattacks have a substantial economic impact that can derail India's growth trajectories, and possess the potential to destabilise the country and make it vulnerable to enemy attacks specifically in conflict areas. In light of this emergent reality, any prospective legislation must account for the increasing number of cyber security issues facing India today. The modern cyber law must formulate strong cyber security provisions and help create resilient regulatory frameworks for the cyberspace that helps India in achieving digital sovereignty.

**v.** ***E-Governance****:* The seeds of a digital India were sown in the late 1990s and early 2000s through a diverse set of Central Government schemes. However, the benefits of these schemes were not fully optimized due to inadequate technical bandwidth. With the *Digital India* programme providing a combined vision and a comprehensive execution plan that enables monitoring of various programmes by the Central Government and offers enhanced technical bandwidth, the government has steered toward realizing the full digital potential of India. Therefore, it is recommended that modern cyber law must provide for enabling provisions that further the *Digital India* initiative and help government agencies and departments provide public services electronically at grass root levels. In doing so, appropriate safeguards must be put in place for providing alternatives means for access to public services to ensure that there is no denial of public services on account of a person's inability to access or use the internet, IT infrastructure, or devices.

**vi.** **Ex Ante Law –**As the technology is ever changing and evolving at a rapid rate. We need to have ex ante cyber laws ready to meet the upcoming challenges. *Ex ante* means 'before the event'. It implies that before any cyber incident or challenges has occurred, the lawmakers must predict what may be the risk and impact of any activity that involve usage or dealing with technology and address those risk areas prior to the incident has happened.

vii. **Minimalistic approach to making of the cyber laws –** Cyber laws should be drafted in such a way that they shouldn't be gigantic which may make it difficult to implement in practical. In India, the process of amending the law is time taking and looking at the dynamic nature of technology, we can't afford to wait for more than a year to amend the law to tackle an issue in the cyber world. A lenient approach should be adopted where the basic principles, obligations, crimes and accountability are provided in the act and specific areas and particular point of concerns must be dealt via rules, regulations, code of ethics and standards which are easier to amend.

**Recognising Emerging Trends and threats in the Cyber space and providing recommendation for combating the Issues -**

The "Fourth Industrial Revolution" is dedicated to technological development which has led to emerging policies and normative issues arising in the cyberspace. These technological advancements are seen across various fields, such as artificial intelligence, digital market, privacy and cyber security, e-governance to name a few of them. This technological advancement revolves around handling data or information in one or the other way. These changing dimensions have brought disruptions in the society and affected social and economic ends and has placed threats and challenges before us. It is extremely hard for the government to regulate the digital sphere as a whole as the rate of change of technology is unimaginable and beyond control and it is spread of various sectors. Hence, separate areas are recognised below and attempt is made to provide recommendation to combat the issue –

a. ***User rights*** – One of the key emerging issues in cyberspace governance is the framework of rights and obligations pertaining to interactions between individuals accessing the internet and availing digital products and services, i.e., users, and entities that control, provide or otherwise supervise these digital products or services directly or indirectly, i.e., digital operators, both public and private.

   User interactions with digital operators presently suffer from certain identifiable vulnerabilities, which include (a) informational asymmetry against users, (b) security breaches, (c) discriminatory treatment in the availability and accessibility of digital products and services, (d)use and deployment of emerging technology such as artificial intelligence while making significant decisions regarding users, (e) targeting of users based on certain protected attributes and the manner of their online interactions, (f) lack of effective grievance redressal mechanisms, and (f) lack of operational frameworks that shall ensure continued access to content preserved in a digital medium to a user's nominated choice after his death. In order to address these vulnerabilities, it is recommended to adopt such a rights-based framework. Such a framework shall offer sufficient protection to user interest and well-being while aiding them in effectively navigating digital advancements and newer technologies. The recognition of such user rights will beneficial to development of law within evolving technological contexts. Hence, such rights be appropriately and succinctly in the modern laws to ensure that the interests and well-being of Indian citizens are central to the application and future development of the law.

*b.* ***Accountability of digital actors*** – The present laws has not kept pace with the changing market realities and the exponential growth in the types of digital business models and actors and the products and services that are being offered by them. The doesn't cover within its scope such new business models and operations and also does not recognise digital actors on the basis of their role and impact in the everyday lives of

citizens in availing essential services. Some digital operators have assumed a scale that distinguishes them from other digital operators. Their large-scale operations have led them to assume dominant positions in the market. They are able to exert this dominance, both vertically and horizontally, across various markets. For example, in the e-commerce sector, very few large entities that exert dominance exist and act as an entry barrier thereby limiting the ability of small players to fully penetrate the market. Therefore, it becomes necessary to create an enabling environment that allows more service providers to enter the market and afford users with different digital services and products. Given the reach of many such dominant digital operators, they also have the ability to cause significant negative impacts and limitations on the rights and interests of users. For example, many global social media platforms have time and again been recognised for the role they play in shaping political discourse and conversations around issues of public interest. Lack of recognition of such differences amongst digital actors hampers effective regulation. A one size fits all approach is not suitable given that constant innovation is leading to myriad digital entities, content, activities, transactions and engagement models. Current enforcement mechanisms are also found wanting. Therefore, there is a need to identify the digital actors and the products and services intended to be regulated, specify obligations accounting their unique functions and characteristics, and have the ability to enforce these obligations effectively. However, in attempting to regulate the digital actors, it must be ensured that the same is done in manner that affords an enabling environment for digital actors to grow in a safe and transparent manner.

c. ***Protection of Privacy and Data*** **-** Given the cross-cutting and cross-sectoral implications of privacy and data protection, it is necessary to have effective regulation and timely intervention. This would require a regulator, an inquiry agency and an adjudicatory mechanism. It is proposed that the IITA establish a dedicated and specialized regulator, inquiry agency and adjudicatory framework for all issues emanating from cyberspace. It is proposed that the modern cyber law establish a dedicated and specialized regulator, inquiry agency and adjudicatory framework for all issues emanating from cyberspace. There may be a dedicated separate data privacy legislature which must establish a dedicated and specialized regulator for cyberspace that possesses multi-disciplinary expertise including in the fields of information and communication technologies, emerging technologies, cyber security, privacy, data protection, and related fields in order to better understand and respond to emerging technological needs of the digital ecosystem. Since data and information are considered the foundational blocks of this ecosystem, the efficiencies that would be derived from a unified regulatory architecture and converged decision-making cannot be ignored. This unified structure will also help address the issues vis-à-vis inter-ministerial and inter-departmental coordination which currently limits timely and effective regulation of overlapping issues.

d. ***Online harms*** – The present IT Act recognises certain types of online unlawful behaviour in the digital ecosystem, it is necessary to provide a holistic framework that recognises online harmful behaviour or information that are distinct from behaviour that is not as yet found to be criminal There are instances where the conduct even though not per se illegal may still cause serious harm to users and society at large. To this end, adopting a harms-based approach to regulation shall help create a responsive framework that accounts for harms that a user might suffer by way of their accessing the digital ecosystem. In taking such an approach, users will be able to initiate complaints with digital operators in such instances, thereby affording a higher degree of control to users to protect themselves more effectively and allow digital

operators to crack down on harmful behaviour. In order to effectively prevent online harms in a changing context, we require a clear regulatory framework that defines harms, places well-defined obligations and provides effective remedies. Such a framework should be user-centric which regulates conduct and information which may not be unlawful per se but is still harmful and is in contravention of modern cyber law. The purpose of taking such an approach is two-fold. First, it allows addressing vulnerabilities to user rights and interests even if they do qualify as a criminal offence; and second, it allows individuals to take a less formalised approach towards redressal, which could lead to a quicker resolution. To this end, it is important to provide for a wide definition of 'harm' which accounts for physical, mental, social, financial aspects that may be caused by any person, including a digital operator. An illustrative list of such harms may include personal harms such as bodily, mental and reputational harms; financial harms such as those arising from theft, extortion, impersonation, loss of employment; discriminatory treatment resulting in effects such as denial/withdrawal/unequal access to service and hindrance in exercise of legal rights such as restriction placed on speech, movement or decision making.

e. ***Cybercrimes*** - Recent estimates indicate an increase in the rate of adoption of internet and digital technologies in India. This increased adoption of the internet coupled with the advent of government initiatives such as Digital India and the Smart Cities Mission - that have brought about a paradigm shift in connectivity and delivery of services, has led to the emergence of new forms of threats and vulnerabilities in cyberspace that now apply to both the urban and rural eco-system. Furthermore, the nature of some traditional offences or crime types has been transformed by the use of computers and other information communication technologies in terms of their scale and reach. New forms of criminal activity have also emerged that target the integrity of computers and computer networks such as the spread of malware, ransomware, and hacking. Government launched cybercrime reporting portal *(www.cybercrime.gov.in*) and there has been steady rise in reporting of cybercrimes with an official record of more than 50,000 cyber cases being reported across the country with predominant motives behind cybercrimes being fraud and sexual exploitation. The risks and harms associated with these offences extend to many aspects of social life such as financial transactions, sexual harassment and other sexual offences, harmful online behaviour and detriment to businesses and their operations. Hence, it is critical to develop legislation that addresses such increased scope and reach in order to mitigate the impact of such offences. India also has largest population using digital technologies and smartphones but many lack awareness [4] of how to avoid cybercrime and do not follow best of digital etiquettes.

   In light of the above, it is recommended that cybercrime be understood as an umbrella term that covers two distinct but closely related criminal activities; cyber-dependant and cyber-related crimes. The distinction is based on the fact that cyber-dependant crimes can only be committed by using a computer resource, computer network or other information communication technologies such as the spread of viruses and other malicious software, hacking and distributed denial of service attacks i.e. the flooding of servers to take down network infrastructure or websites, whereas cyber-related crimes are traditional crimes that are increased in their scale and reach by the use of computer resources, computer networks or other information communication technologies such as fraud-(including mass marketing, phishing emails and, online banking and e-commerce frauds), theft- (including theft of personal information, personal data), sexual exploitation of children and adults and the spread of misinformation or disinformation. Therefore, it

is proposed to review and reformulate the offences under the IT Act as well as to consider recognising and introducing emerging and new forms of cybercrimes including revenge revenge pornography, cyber stalking, fraudulent collection of personal data, targeted spreading of disinformation or malicious communication with the intent to cause alarm amongst the public in line with developing international jurisprudence and the socio-economic and political realities of India.

f. **e-Governance** - Governments across the world have rapidly adopted information technology and related service for the facilitation and provision of public services to their citizens. India too, through the government's Digital India programme has launched massive e-governance schemes such as Aadhaar, Digi Locker, PayGov, myGov.in. Additionally, the onset of the Covid-19 pandemic has amplified the need of making public services available electronically in a holistic, non-discriminatory, and inclusive manner. The modern cyber law must guarantee o public services. It must recognise that while providing e-governance services, no person is denied access to public services due to their inability to access, use or understand the internet, information technology, devices, or IT infrastructure and that there are no un-intended consequences of delivering public services electronically. In furtherance of this objectives, it is proposed to provide basic protections in relation to electronic service delivery under modern cyber law while prescribing e-governance standards and ensuring the protection of personal data. These may include requiring simple and easily understandable forms and processes, increasing accessibility of services and creating viable alternative means to prevent technological exclusion. It is also noted that the need to statutorily recognize the involvement of third-parties in offering technical solutions to enable public service delivery and proposes the introduction of provisions specifically catering to the same in modern cyber law.

g. ***Notifying more forensic labs under Section 79A of the IT Act*** – Last year the Ministry of Electronics & Information Technology notified two forensic laboratories as the 'Examiner of Electronic Evidences within India'. The scope of both the laboratories extends to computer (Media) forensics excluding Floppy Disk Drive and Mobile Devices Forensics. Such body corporate shall provide an expert opinion on electronic evidences before any court or other authority. Many other forensic laboratories of similar nature are in demand with much wider scope to support the electronic evidences. As technology is promoted everywhere and so as in forensics, it calls for government initiatives to notify other forensic laboratories as well.

**References**


1. Growing Cyber Threats for Digital India Kaspersky Report https://www.kaspersky.co.in/about/press-releases/2021_the-growing-cyber-threats-for-digital-india-kaspersky-report-reveals-that-35-of-indian-online-users-were-attacked-by-web-borne-threats-in-2020
2. Cyber Crime Motives 2020 https://ncrb.gov.in/en/crime-in-india-table-contents?page=43
3. Page 5, "Online Harms White Paper", HM's Government, United Kingdom (2019) available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf.
4. **Cyber Unsafe,** A Handbook for Preventing Computer Frauds and Cyber Crimes by **Gaurav Gupta | Garima Gupta,** vilvam publications, ISBN: 978-81-954229-1-3

# Chapter 4

## Transparent and Real-time Grievance Management System

*Author - Dr. Ramanand N. Shukla, Quality Council of India*

### Governance and Grievance Management

The concept of "governance" is age old which has helped the human civilization evolve and take shape into its current form. In simple words, Governance is a process of managing affairs, at different levels and can be used in various contexts such as national governance, local governance, corporate governance, etc. According to UNDP, Governance is defined as "the exercise of economic, political, and administrative authority to manage a country's affairs at all levels. It comprises mechanisms, processes, and institutions through which citizens and groups articulate their interests, exercise their legal rights, meet their obligations, and mediate their differences."

As governance is the process of managing affairs, it implies that the it should ensure welfare of the stakeholders through a participatory approach. The practices that help to strive for the welfare of its stakeholders form the basis of good governance.

The United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP) identifies following eight principles of 'Good Governance', in reference to the political or governmental governance:

1. Participatory
2. Accountability
3. Transparency
4. Responsiveness
5. Consensus-orientated approach
6. Equitability and inclusiveness,
7. Consistency with the rule of law, and
8. Effective and efficient

These eight principles lay down the foundation of Good governance. Out of these, the first six principles are about involving the citizens and other stakeholders in decision making process for effective management. One of the key indicators of this proactive involvement is a mechanism of effectively managing the 'grievances' of the citizens and other stakeholders.

The term 'grievance' has its origins in the Latin word 'gravis' meaning 'heavy' which refers to a hardship suffered, which may elicit a negative feedback or complaint. A grievance is a concern, problem or claim, which may be perceived or actual, that an individual or group looks forward to be heard, have it addressed and resolved, as the case may be. In political or governmental parlance, a grievance is a complaint lodged by a citizen or another stakeholder towards the government or services of government institutions due to dissatisfaction or hardship suffered. These grievances or complaints can become an important tool for the decision makers, governments and their agencies to evaluate the effectiveness and efficiency of their programmes, mechanisms, processes, and institutions. In other words, 'grievance management' of the citizens and other stakeholders can be effectively used for performance evaluation of a government which is also stated under the sub goal 16.6 of Sustainable Development Goal (SDG) 16 of the United Nations.

#### Effective Grievance Management System

An effective grievance management system has a great intrinsic value. First & foremost, it gives voice and equal opportunity to get heard, to the marginalized. Second, it instils trust and respect among the citizens and stakeholders towards the governance. Third, it instils sense of accountability among the agencies and officials.

Fourth, it deters corrupt practices by providing a secure platform for the aggrieved as well as the whistle-blowers. Finally, it provides timely insights and early warning on the ground realities to the decision makers for improving effectiveness and efficiency of the programmes and services. Grievance management system therefore, is not only a key indicator of how good is the governance is but an instrument to enhance effectiveness and efficiency of governance.

However, the system will lose its intrinsic value if the system is slow with a lag in redressal of the public grievances and is unable to provide a real-time feedback to the decision makers. Today's era of technology has made it possible to create systems that could help in real time monitoring and feedback enhancing the effectiveness of the grievance management system.

## Features of an effective Grievance Management System

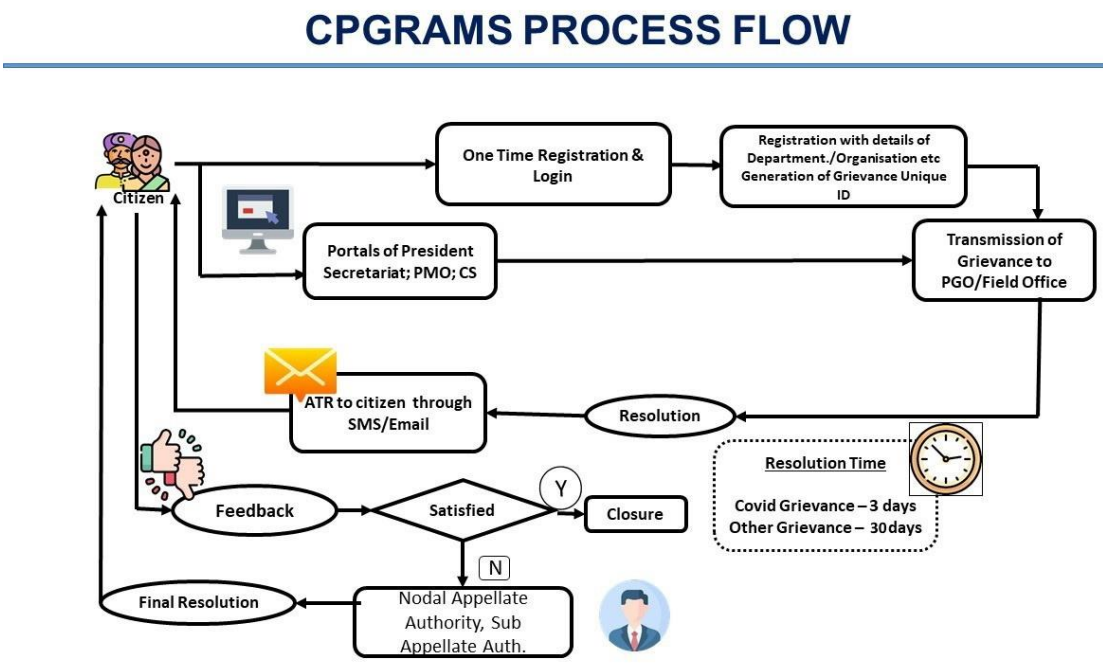
- **Awareness**: The grievance management system should be widely publicized to ensure awareness amongst all the citizens and stakeholders
- **User friendly**: The system should be designed to be user friendly for everyone including those with special needs
- **Accessibility:** The system should be accessible to everyone irrespective of their background, literacy levels, disabilities, geographical locations, etc.
- **Transparency**: The system should be transparent enough to let the citizens and stakeholders understand how decisions are reached
- **Confidentiality**: The system should be designed to ensure safety and rights of all stakeholders who use the system by ensuring anonymity, where needed and/or protection to the aggrieved
- **Fairness**: The system should be based on the principles of impartiality and independence to ensure a credible and objective approach to address the grievances without any external interference
- **Real-time responsiveness**: It should be ensured that grievance management system is responsive to address the grievances in an efficient and time bound manner.
- **Closed loop system:** The system should ensure that the loop is closed by ensuring redressal of the grievance, feedback of the aggrieved/complainant on the resolution and providing timely inputs to the decision makers on the underlying problems or the root cause to eliminate recurrence of similar issues or concerns
- **Review of the system:** The grievance management system should also have a process of an independent review to ensure that the system works effectively and efficiently to achieve the objectives

### CPGRAMS – The Grievance Management System of India

Centralised Public Grievance Redress and Monitoring System (CPGRAMS) is the 24x7 online platform for the citizens to lodge their grievances to the public authorities on any subject related to service delivery. It exhibits most of the features of an effective grievance management system. It has been designed as a single window system which is connected to all the Ministries/Departments of Government of India and States where every Ministry and States have role-based access to the system. CPGRAMS is also accessible to the citizens through standalone mobile application downloadable through Google Play store and mobile application integrated with UMANG.

CPGRAMS portal provides important information including the timelines for resolution of different types of grievances/complaints.

The system also allows to track status of the grievance filed with the unique registration ID provided at the time of registration of the grievance or complaint. It also provides a provision/facility of appeal to the citizens if they are not satisfied with the resolution by the Grievance Officer. After closure of the grievance, the complainant can also provide feedback.




***Source**: pgportal.gov.in*

## Conclusion

Good governance is an ideal concept to achieve the goal of a just, peaceful and inclusive society. The policies and interventions of the government may exhibit the intent of good governance, however, it is the citizens who are the ultimate judges of a government's performance. An effective and transparent grievance management system which addresses citizens' grievances in in a time-bound, manner providing a satisfactory resolution, cements the government's good governance credentials.

Having an effective grievance management system doesn't mean that it will end all the issues and grievances forever. Grievances will keep coming and they must be considered as an opportunity to continually improve the effectiveness and efficiency of the government institutions and their services to further the objectives of good governance. An effective grievance management system therefore should be seen as a key component of a good governance.

**References**

https://www.unodc.org/e4j/zh/anti-corruption/module-2/key-issues/what-is-good-governance.html
https://www.unescap.org/sites/default/files/good-governance.pdf
https://pgportal.gov.in
https://www.un.org/sustainabledevelopment/peace-justice

# Chapter 5

## 21st Century Digital Infrastructure for next-generation Services and Security in Cyberspace

Author - Vivek Roy – Business Segment Head for Digital Connectivity & Power at Siemens Limited, India.

### A backbone of our society

Digital connectivity is making our lives easier and boosting business competitiveness. However, the risk of cyberattacks is increasing as well. How to meet this challenge?

***We do not realize just how dependent we are on digitalization until something goes wrong – something like an attack launched by a horde of hackers. For this reason, cybersecurity acts as the fundamental basis of the efficient and long-range advancement of our society.***

There was something fishy going on here. The cursor in the control system of the water treatment system of Oldsmar, Florida, seemed to be guided by an invisible force. The IT specialist who was overseeing the operation watched as the amount of sodium hydroxide, a chemical used to regulate acid levels, shot 100 times above its normal level. The IT specialist at the waterworks realized one thing right away: A hacker had struck. The employee then had to do some fast thinking on his feet: Once he had wrestled back control of the system, he lowered the level of the chemical back to normal levels. The plant operator announced that the incident posed no danger to the community of 15,000 residents. It also noted that it would have taken 24 hours for the contaminated water to have reached households and that an automatic alarm would have sounded long before then.

The incident that occurred in Oldsmar in February 2021 can repeat itself anywhere at any time – and possibly have much more serious consequences. It also illustrates just how dependent we are on a smooth-running system that supplies us with food, water, energy, information, mobility services and healthcare – and just how vulnerable these infrastructures truly are. Digitalization is both a blessing and a curse. On the one hand, it facilitates a highly efficient system that meets the growing needs of our civilization – things like smart homes, medical centers, train travel, production and, of course, water supplies. No matter where you look: Nothing works without digitalization. On the other hand, our vulnerabilities are well known to criminal hackers, individuals who are out to extort money or destabilize countries – and are able to wreak havoc in our daily lives rather easily.

**MORE LIKE A MARATHON THAN A SPRINT**

For this reason, cybersecurity is not an optional, nice-to-have feature of digital technology. Rather, it is a fundamental pre-condition for public services and high standards of living for everyone, services and standards that are achieved while using as few natural resources as possible. “Digitalization and cybersecurity have to be friends,” says Christian Paulsen, the Product and Solution Security Officer at Siemens Mobility.

*Train station Deutz/Cologne: Particularly in long-term transportation system projects, it becomes apparent that hardware ages, but software does not. Accordingly, the life cycle must be considered holistically in order to ensure adequate cybersecurity.*

Cybersecurity is a job that resembles a marathon more than a sprint. It is a fact of life that Paulsen’s colleagues at Siemens Mobility know only too well. They think in terms of decades when they tackle such jobs as upgrading the signal system of a rail line. Such service contracts usually run for 30 years. The hardware may wear out, but the software does not. Nonetheless, it will turn into a security risk if it is not updated. This is the problem that nearly led to a disaster in Oldsmar. The water treatment plant was using a Windows 7 operating system. In addition, the simple password used to gain access to the system was never reset.

It was an approach that was much different from the holistic security concept that Siemens uses for transport systems, a strategy that consists of a wide range of measures. Two key factors come into play here: The concept must be seamless and holistic. It must also be used throughout the entire life cycle of a product, from development and installation to operation and decommissioning. This effort includes regular updates, penetration tests designed to analyze vulnerabilities, secure data connections, transparency extending across all measures, rapid responses to security breaches and much more. “By taking this approach, products can maintain their youth even as they age;” Paulsen says. “They will also remain secure and can be used for years and years to come. It all boils down to what sustainability is all about.”

**A MATTER OF LIFE, DEATH, AND GOOD HEALTH**

Every business field takes a similar approach. For example, the healthcare sector, where the challenges are especially great. The number of cyberattacks launched against the healthcare system has climbed nearly 30% during the pandemic. One reason for the increase is the expanded number of targets now available to hackers, a rise attributed to the expanded number of online services that have arisen as a result of remote working by

healthcare employees. Hackers are also increasingly exploiting the pressure faced by healthcare providers to exhort money with the help of ransomware. Cybercrime is a business. “The healthcare sector clearly demonstrates that cybersecurity is a necessity and is thus a sign of quality,” says Carlos Arglebe, the Head of Cybersecurity at Siemens Healthineers.

Protection for IT systems and data assets: Cybersecurity is essential in hospitals.

It can even amount to a question of life and death. Last year, for instance, a woman had to be transported by ambulance to the University Medical Center in Düsseldorf. Unfortunately for the patient, hackers had brought the hospital’s IT system to a standstill in a bid to extort money. As a result, the ambulance was redirected to a hospital in Wuppertal, a city located more than 30 kilometers away. It was a detour that cost precious time. The woman died. Her death was probably not the result of the hacker attack – but the incident clearly illustrates the potential threat that hacker attacks pose to hospitals.
The attack carried out over a period of several days had other far-reaching effects on the hospital as well: The Düsseldorf medical center was able to admit only half the number of patients that it normally does. Its surgeons were able to perform a maximum 15 operations each day instead of the normal number of up 120 procedures. Unfortunately, such cases are occurring more frequently throughout the world.

**SECURE SUPPLY CHAINS**

But all of this hard work means little if suppliers cut corners on security. Secure supply chains are one of the principles contained in the Charter of Trust that Siemens initiated in 2018 and that now comprises 17 companies. As a result, new suppliers of charter members like Siemens must observe binding minimal requirements imposed on cybersecurity. These requirements are spelled out in a mandatory clause contained in all new contracts. The Charter of Trust is composed of 10 principles that contain recommendations for improved cybersecurity, including enhanced training and regulatory conditions.

The principles serve as the big picture. In doing so, they expand the horizons of cybersecurity, an area that is still largely confined to technical measures. But they are a means to an end: like the sustainable development of our civilization and our planet

# Chapter 6

## Shifting the Gear on Emerging Technologies from Exploration to Population Scale Solutions

Authors - Dr Gaurav Gupta, Scientist 'E', Ministry of Electronics and Information Technology

&

Dr Garima Gupta, Independent Researcher, Post Doc, IIIT Delhi

**Abstract**

Creativity and Innovation are critical to the future well-being of society and to driving economic growth. The disruptions brought by technology innovations help society and world move forward creating new opportunities. Today, various stakeholders around the world in the field of design, development and deployment are innovating and striving hard to ensure emerging technologies see population scale solutions and many such success stories are already seen by the world specially during covid times. World leveraging digital technology to roll out biggest vaccine management program through CoWin to shifting supply chain alternatives in India. Adoption of Artificial intelligence, machine learning, IoT, cloud and mobile technology is shaping the future. The world is also seeing dependencies on cyber world leading to instances of cyber-crime and cyber incidents highlighting the need of cyber security and digital forensic investigations.

Key Words: Emerging Technologies, Cyber Crime, Digital Forensics, Disruption.

## 1. Emerging Technologies and Disruption based business Models

A business model that can link emerging technology to an upcoming market need is the key to industry transformation. One usually associate transformation of businesses with the adoption of emerging technologies. Although emerging technologies are often major factors, they alone have never transformed an industry on their own. What does achieve such a transformation is a unique business model that can link a emerging technology to an upcoming market need. For example, MPEG Audio Layer-3 (MP3) based devices represented an order-of-magnitude increase in capacity over magnetic tapes and CDs. With introduction of MP3 users could carry hundreds and thousands of songs on a small device. But MP3 players revolutionized the audio devices market only after Apple coupled the iPod with iTunes in a new business model, swiftly moving music-recording sales from the physical to the virtual world. When Apple coupled the iPod with iTunes, it revolutionized the audio devices market. Similarly, UBER, which upended car rental industry and Airbnb, which upended the hotel industry and amazon which has upended shopping industry. These tech companies have experienced phenomenal growth: They now have more rides / rooms/ shopping items than either taxi providers / hotel industry / shopping malls. The founders of these tech companies realized that platform technology made it feasible to craft an entirely new business model that would challenge the traditional economics of the existing business. Unlike conventional hotel chains, Airbnb does not own or manage property—it allows users to rent any livable space (from a sofa to a mansion) through an online platform that matches individuals looking for accommodations with home owners willing to share a room or a house. Airbnb manages the platform and takes a percentage of the rent. Similar is the case with UBER and Amazon. Since income of these technology companies

does not depend on owning or managing physical assets, they do not need large investments to scale up and thus can charge lower prices (usually 30% lower than actual charge). Moreover, since the home owners / taxi drives and merchants are responsible for managing and maintaining the property / taxi and merchandise and any services they may offer, the tech companies risks (not to mention operational costs) are much lower than those of traditional service providers. On the customer side, technology company model redefines the value proposition by offering a more personal service—and a cheaper one. Before platform technology existed, there was no reason to change the hotel/taxi/merchandise business in any meaningful way. But after its introduction, the dominant business model became vulnerable to attack from anyone who could leverage that technology to create a more compelling value proposition for customers. The new business model serves as the interface between what technology enables and what the marketplace wants.

## 2. Features that make a business model transformative

Following features usually correlated with a higher chance of success at transformation in any new business initiatives where technology played an important part.

- **Personalized product or service.**

  Many new models offer products or services that are tailored made than the dominant models to customers' individual and immediate needs. Companies often leverage technology to achieve this at competitive prices
- **A closed-loop process.**

  Many models replace a linear consumption process (in which products are made, used, and then disposed of) with a closed loop, in which used products are recycled. This shift reduces overall resource costs.
- **Asset sharing.**

  Some innovations succeed because they enable the sharing of costly assets—Airbnb allows home owners to share them with travelers, and Uber shares assets with car owners. Sometimes assets may be shared across a supply chain. The sharing typically happens by means of two-sided online marketplaces that unlock value for both sides: I get money from renting my spare room, and you get a cheaper and perhaps nicer place to stay. Sharing also reduces entry barriers to many industries, because an entrant need not own the assets in question; it can merely act as an intermediary.
- **Usage-based pricing.**

  Some models charge customers when they use the product or service, rather than requiring them to buy something outright. The customers benefit because they incur costs only as offerings generate value; the company benefits because the number of customers is likely to grow.
- **A more collaborative ecosystem.**

  Some innovations are successful because a new technology improves collaboration with supply chain partners and helps allocate business risks more appropriately, making cost reductions possible.
- **An agile and adaptive organization.**

  Innovators sometimes use technology to move away from traditional hierarchical models of decision making in order to make decisions that better reflect market needs and allow real-time adaptation to

changes in those needs. The result is often greater value for the customer at less cost to the company. Each feature on this list is tied to long-term trends in both technology and demand. On the tech side, one trend is the development of sensors that allow cheaper and broader data capture. Another is that big data, artificial intelligence, and machine learning are enabling companies to turn enormous amounts of unstructured data into rules and decisions. A third is that connected devices (the internet of things) and cloud technology are permitting decentralized and widespread data manipulation and analysis. And a fourth is that developments in manufacturing (think nanotechnology and 3-D printing) are creating more possibilities for distributed and small-scale production.

All six features represent potential solutions for linking market demand and technological capability. For example, greater personalization in the value proposition responds to the fragmentation of consumer preferences and the resultant demand for more-diverse offerings. That personalization has been made possible by sensors that collect data from connected devices via the cloud; the data is analysed by big data solutions and turned into services—such as recommendations and alerts—that are different for each user. CoWin application to roll out vaccine to all Indian is one such famous example that ticks almost all the feature mentioned above realising success of the application.

## 3. Potential for Use as well as Misuse of AI, ML, Big Data

Technology is 'Agathokakological', that is, consisting of both good and evil. Technology has always been seen as a double-edged sword, starting from nuclear (from energy to bombs) to now digital technology (from a connected world to cyber-crimes). Technology has always evolved to solve a pending issue, and the evolution of technology should provide more convenience to mankind. But there have always been criminals, who misuse technology to carry out illegal activities. Most technology is met with initial euphoria leading to mass adoption and then misuse by criminals. Similar is the case with digital technology. In a very short span of time, digital technology has changed the way mankind lives today, a world where everything is available at the click of a mouse. In today's digital world, your data is more valuable than you can imagine. We are at that point of time in the evolution of digital technology when, if timely interventions are not made, the misuse of technology will become rampant that it will soon become a bane.

Cyber security risks are growing exponentially. The World Economic Forum's global risk report has been highlighting cyber security risk as one of the top five risks to mankind for the past few years. It is no longer a minor concern, but has become one of the largest organized crimes. While enterprises and governments are comparatively better prepared to deal with this, it is the individuals, who are more vulnerable and can easily fall prey to such attacks. With exponential digitalization of our lives and increased contact-less dealings due to the pandemic, the cyber-crime involving the general people is on the rise. People can lose a lot of their money, their data, their reputation, and much more, as a result of a cyber-attack. People also have limited familiarity to detect and deal with a cyber incident, and the lack of published information about how these crimes are committed makes it very hard for people to safeguard themselves. Although digital technology has the potential to shape the future of mankind it comes with many worries that never existed before. Some of these include:

- Eternal and immortal digital data which exists forever.
- Information becoming viral at unimaginable speed and with an unrestricted reach, leading to instantaneous fame (or infamy) in a few clicks in a few seconds.

The use of technology demands exemplary discipline and control, which the majority of the population does not possess, leading to consequences beyond human thought. Artificial intelligence, machine learning, cloud and IoT coupled with 5G creates a world of opportunities for cyber criminals. In today's work everything including audio, video, image, document and product can be made synthetically leading to serious potential of damage both in terms of reputation as well as economically. Computer frauds and cyber-crimes are, therefore, the greatest threat to every individual and business in today's world.

## 4. Peeking into future of emerging technologies and need for development of sustainable population scale solutions

Mankind dependence on Artificial intelligence, machine learning, cloud and IoT coupled with 5G will increase continuously and most of cyber-crimes and cyber security incidents are avoidable by practising digital etiquettes and cyber-crime awareness is the key. Cyber Unsafe [1] is such an effort in this direction. [1] details how technology fraudsters are exploiting digital technology and its users and highlights the concepts of digital hygiene. It is anticipated that digital technological crime exploding human emotions, sensory capabilities will increase and criminals syndicates will exploit technology on large scale including following methods:

Computer frauds and cyber-crimes are a classic Example of how digital technology can provide new dimensions To traditional crimes and make them more sophisticated. With ever-increasing reliance on digital technology, the number of digital crimes has been growing exponentially. Lack of public awareness of the potential misuse of digital technology is further fuelling the growth of these crimes. There is very little reliable information available to help people understand the dangers associated with digital technology. This talk is an attempt to fill this gap. How the future of digital crime is shaping and what is expected from LEA, Judiciary, Forensic labs and academia stakeholders ensure cyber safe world with relatable stories, revealing facts, and incisive insights, Cyber Unsafe busts the many myths surrounding digital technology and related crim

- We are already witnessing ransomware attacks, bot attacks along with malware stealing data and information from computing resources.
- Side channel attacks including information leakage through sensors of mobile phones, wearables are becoming prevalent.
- Crime against techno shy senior citizens are also increasing.
- There is lack of trained manpower to handle cyber security, incident management, cyber lawyers, trained law enforcement agencies and digital forensics investigators and this itself presents a large scale opportunity needing immediate solution. Cyber-crime could be the biggest job creator over the next decade for criminals as well as for law enforcement agencies, investigators, forensic experts, lawyers, and judges. For example, new job profiles such as accessors to evaluate digital forensic readiness, chief security and digital forensic officer (CSDFO) for enterprises, educators in the domain of digital and cyber forensics, and enterprise forensic lab professionals to provide digital forensic services on demand to people across the world are likely to emerge.

- Technology is used by criminals to carry out conventional crimes in a more effective manner. Many traditional crimes, earlier carried out in person, are now being aided, enhanced, or abetted through the use of technology. Stalking and bullying is now done online where the perpetrators can reach their victims twenty-four hours a day, seven days a week.
- Identify frauds and counterfeiting of documents have become possible due to the advent of good quality and economical scanners and printers, making the counterfeit documents extremely realistic. The registers in visitors' parking lots, data with mobile recharge vendors, and parking stickers on car windscreens carrying house and phone numbers are mined and then misused using social engineering. There is no easy way to file a complaint about the fake websites that take orders and money by promising deals but never deliver the product.
- Smartphones are the greatest example of convenience through convergence and, at the same time, they are also the greatest nuisance. The users of technology believe in convenience and will do what they want to do with technology. Technology developers have to stop blaming them for security failures and develop solutions which account for user imperfect behaviour. This convergence for convenience provides easy opportunities for criminals to exploit billions of unaware, uninformed, and innocent users of digital technology for malicious and unlawful gains. The most unaware users are easy prey, like sitting ducks waiting to be exploited by fraudsters. The amount of information stored on a smartphone has skyrocketed in recent years. The abundance of apps means we supply nearly every piece of information about ourselves, whether it is bank account details or our preferred taste in pizza to the apps present on our phones. For a cyber-criminal potentially wanting to commit identity theft, a smartphone is a goldmine. Further, the concept of Bring Your Own Device (BYOD) has become one of the most prominent trends for companies around the globe. Cyber criminals are viewing these devices as an ideal gateway into stealing valuable corporate information.
- Fake news' virality is six times more than genuine news'. Fake news fetches more hits to websites, and thus more revenue. Starting from misinformation related to home remedies for the treatment of Covid-19 to post-demonetization news about 'spying technology' added to the banknotes of INR 2000 denomination and misinformation leading to a mob killing, fake news circulation is the major subject of WhatsApp University. Everyone thinks they are experts just by reading a forward they received on WhatsApp. Older people are more susceptible to believing WhatsApp-based news. They almost believe it blindly and act as the main propagators. They are, thus, used as targets to spread more fake news. Fake news makes real money as users are attracted to them. There are instances of violence-inciting fake news, election propaganda, and hate speeches being circulated on WhatsApp. The scale of the problem of fake news is overwhelming and requires a multi-stakeholder approach to contain it.

Thus, technological enhancements are cleverly used for committing both conventional as well as modern crimes effectively and efficiently. The methods and techniques used by criminals are constantly changing; they will mutate, and new, unseen variants will keep raising their ugly heads, posing a serious challenge to technology users. Further, Availability of economical, technologically enhanced hardware has led to the development of solutions which leverage artificial intelligence and predict the user's psychology, leading to addictive behaviour. The ultimate aim of all service providers is to grab the user's attention and keep them glued to the screen in

order to earn maximum profit by selling data or showing advertisements. There is a race between companies to develop artificial intelligence-based attention seeking algorithms leveraging the neuroplasticity of the brain that leads to addiction (digital dopamine). As per a study conducted by NIMHANS, 73 per cent of teenagers in urban India are affected by 'psychiatric distress', and overuse of digital technology has been cited as one of the major reasons impacting mental and physical health adversely. SHUT (Service for Healthy Use of Technology) is one such initiative by the National Institute of Mental Health and Neurosciences Centre for Well-Being helping manage technology addiction. Discrimination based on digital behaviour is real and will have far-reaching impacts on mankind**.**

**In summary, we can say that shifting the gear on emerging technologies from exploration to population scale solutions is possible by adopting awareness and by ensuring security of digital technology while big tech companies use the cyber space responsibly to make the *internet* "*open*, *safe* and *trusted*".**

**References**

Cyber Unsafe**,** A Handbook for Preventing Computer Frauds and Cyber Crimes by Gaurav Gupta | Garima Gupta**,** vilvam publications, ISBN: 978-81-954229-1-3

# Chapter 7

## The Role of E- governance in bridging the Digital Divide

Author - Shishir Bharadwaj- Advisor, Quality Council of India

Digital divide refers to that disparity between individuals and/or communities who can use electronic information and communication tools, such as the internet, to better the quality of their lives and those who cannot. This creates a gap that exists between those with ready access to the tools of information and communication technologies and the knowledge that they provide access to and those without such access or skills. This deprivation could keep many needy without access to job or welfare schemes in times of disaster or even getting a passport more expensive. To ensure that such groups are not left out of the government programs, E-governance initiatives will create the infrastructure for delivery funded by the government mandate and also draw most citizens to adopt technology when they see an immediate tangible benefit.

Information and communications technology (ICT) is a key weapon in the war against uplifting a society and delivery of citizen services to every part of the society. When used effectively, it offers huge potential to empower people in developing countries and disadvantaged communities to overcome development obstacles, address the most important social problems they face, and strengthen communities, democratic institutions and local economies.

Yet a digital divide separates those who can access and use ICT to gain these benefits, and those who do not have access to technology or cannot use it for one reason or another. There are a wide range of projects underway aimed at bringing ICT to people in India. But in order for ICT to have a real impact on people's lives, it is crucial that development efforts go beyond computers and connections to ensure that people have real access to ICT so they can use it effectively to improve their lives.

The digital divide is usually measured in terms of the number of telephones, computers, and Internet users. Between groups of people within countries, it is usually measured in terms of race, gender, age, disability, location, and income. It is difficult to gain an overall understanding of the digital divide, the proposed solutions, and what is having a real impact, when there are multiple definitions of the problem, conflicting views on whether it is getting better or worse, and various opinions on the key factors affecting it.

The digital divide is growing around the world, despite the fact that all countries and all groups within countries, even the poorest, are increasing their access to and use of ICT. This is because people in ICT "have" communities and groups are increasing their access and use at an exponential rate. At the same time, ICT "have-nots" are increasingly excluded from jobs, participation in government processes, and public discourse on the issues that affect their lives, leaving them politically and economically powerless.

However, the infusion of ICT can intensify existing disparities. ICT alone is not enough to solve long-standing imbalances and can make inequalities worse if not applied wisely. The digital divide is a complex problem, presenting both practical and policy challenges. It is also apparent that solutions that work in developed countries cannot simply be transplanted to developing country environments: solutions must be based on an understanding of local needs and conditions. An understanding of grassroots realities, pooling of resources, and a favourable regulatory system are among the many elements necessary in an effective approach to the digital divide.

**What is being done?**

Governments, businesses, individuals, and organizations have studied the issues at stake in the digital divide and drafted a range of valuable reports—from statistical analyses to in-depth case studies. Most offer recommendations for tackling the problems, usually suggesting specific ground level initiatives and policy reforms. Many also cover the wider issues that impact on digital divides, such as e-commerce, information society, and healthcare. Numerous on-the-ground initiatives are working to provide technology access and help put technology to use in underserved populations. There are an enormous number of efforts, ranging from projects that create public centers where poor people can use kiosks and computers, to those that incorporate ICT in healthcare, to programs using innovative technology in small business applications. These efforts are

driven by organizations that range from the smallest NGO working in remote areas to the largest multinational corporations, such as Hewlett Packard's $1 billion "E-Inclusion" initiative to promote hardware innovations suitable for developing country environments.

Many initiatives address specific aspects of the range of issues, but too often they neglect related factors that limit their success. For example, too many community access projects providing computers and connections in rural locations do not become self-sustaining because local people do not use their services—often they have failed to address the role of the center in the local economy or the need for locally relevant content. There is a need for a holistic approach to cover the range of issues to create effective and sustainable uses for technology that are integrated into local society.

**What more is needed? Real Access**

Providing access to technology is critical, but it must be about more than just physical access. Computers and connections are insufficient if the technology is not used effectively because it is not affordable; people do not understand how to put it to use; people are discouraged from using it; or the local economy cannot sustain its use. ICT projects will only be widely successful in developing countries when all of the other components necessary for the effective integration of ICT into society are in place. This real access to ICT, looks at twelve interrelated factors that determine whether ICT can be effectively used by people:

• **Physical access**: Is technology available and accessible to people and organizations?

• **Appropriate technology**: Is the available technology appropriate to local needs and conditions? What is the appropriate technology according to how people need and want to put technology to use?

• **Affordability**: Is technology affordable for people to use?

• **Capacity:** Do people have the training and skills necessary for effective technology use? Do they understand how to use technology and its potential uses?

• **Relevant content**: Is locally relevant content available, especially in terms of language?

• **Integration**: Is technology use a burden to peoples' lives, or is it integrated into daily routines?

• **Socio-cultural factors**: Are people limited in their use of technology based on gender, race, or other socio-cultural factors?

• **Trust**: Do people have confidence in technology and understand the implications of the technology they use, for instance in terms of privacy, security, or cybercrime?

• **Legal and regulatory framework**: Do laws and regulations limit technology use? Are changes needed to create an environment that fosters its use?

• **Local economic environment**: Is there a local economic environment favourable to technology use? Is technology part of local economic development? What is needed to make it a part?

• **Macro-economic environment**: Is technology use limited by the macro-economic environment in the country or region, for example, in terms of deregulation, investment, and labor issues?

• **Political will**: Is there political will in government to do what is needed to enable the integration of technology throughout society, and public support for government decision making?

Overall, a pooling of resources and experiences is needed. Dealing with the digital divide is beyond the scope of any single initiative. The funding for E – governance could help create infrastructure while ensuring that digitisation of records and electronic documents quickly replace paper, for example. This will increase the speed of service delivery and also push users to use basic technology that will suffice for such purposes.

Private sector programs and philanthropic efforts are vital too, although there is room for improvement. For-profit programs are successfully expanding access to technology to increasingly larger groups, but often fail to adequately address the needs of the poorest areas and the poor citizens within countries. In isolation they can exacerbate divisions within countries since privileged groups are more able to afford and use the technology.

Donations and philanthropic programs have demonstrated the useful application of technology among underserved populations, but in many cases, they have failed to produce sustainable, widely replicable models.

The digital divide is not a new problem. We should learn from previous experience in fields such as economic development, technology transfer, and sustainable development. Many of these ongoing programs have an impact on the digital divide, and coordination will benefit everyone.

Getting government policy right is also critical.

Governments can play a fundamental role in creating an environment that will foster technology use and encourage investment in ICT infrastructure, development, and a skilled workforce. Government action is also important in spreading the benefits of technology throughout society, and governments have the power and mandate to balance the needs of their citizens for long-term economic growth and social prosperity. However, translating a vision to practical steps that fit the local context is not a simple matter. Leaders need to have a realistic appreciation for what ICT can—and cannot— do for their countries and communities, and they must lead effectively and bolster public confidence in the path they take. A range of projects are underway in India to integrate ICT in a number of critical areas, including education, healthcare, government, trade, and small business support. However, these projects frequently encounter obstacles that directly or indirectly relate to the country's policy environment.

But often at the working level, government officials do not understand the implications of existing policies that may hinder ICT use, nor the changes they need to make to create a more favourable environment. Some governments have subscribed to e-strategies promulgated by outsiders, but at a practical level they lack the political will to drive change because they do not enjoy widespread public support for an ICT-focused approach. Often this is because government officials fail to engage stakeholders in framing the e-strategies, so they do not have public buy-in for their long-term plans. In some cases, the government has partnered with the country's business and civil society sectors to promote ICT enabled development at the ground level, but the various stakeholder groups lack the experience and resources to give effective input. To cross the digital divide and put ICT to effective use to improve people’s lives, countries and communities must be "e-ready" in terms of infrastructure, access, training, and a legal and regulatory framework that will foster ICT use. If the digital divide is to be narrowed, these issues must be addressed in a coherent, achievable strategy that is tailored to meet local needs.

If the E-governance approach could look at changing needs of society and what needs to be done we could reach out to have-not by the below mentioned sample of services.

- National roll-out of tele-medication, including identifying relevant areas, testing new patient groups, and providing the necessary infrastructure;

- Effective collaboration in the healthcare area, including digital booking at hospitals, better user of patients’ own information, implementation of a joint national medication card, fully digital communication in the healthcare sector, increased use of video conferencing, for example for interpretation;

- Welfare technology and care, including the roll-out of devices to help lift patients, washing toilets, use of eating robots in senior housing facilities, digitally supported recovery and testing of smart homes;

- New digital approaches in case handling, including freeing up resources through speech recognition, better evidence in social policies and programmes, and increasing quality through better data sharing;

- Digital learning and education, including using digital teaching aids and educational materials in schools, digital exams, digital tools for day care;

- Using cloud-based services for creating life event-based service deliver where all necessary data is verified and exchanged for seamless delivery of services.

Governments face the challenge of achieving public sector efficiency in general, productivity in the delivery of public services, and effective policies and good governance practices. While digitisation enables new opportunities and reinforces a drive for policy and service transformation in a number of areas, public sector

use of digital technologies should remain driven by clear purposes and value propositions. E-governance could very much deliver all that is expected from it but the risk of digital divide will always limit the reach of the benefits of digitisation. In India we have always created demand and then the infrastructure, maybe this too E-governance could create the demand for reducing the digital to such a level that which could have a quantum impact of quality of life Indians.

# Chapter 8

## Digital Governance for enhancing Ease of Doing Business and Ease of Living

Author - Shishir Bharadwaj- Advisor, Quality Council of India

Ease of living for every citizen of India, probably constitutes most to the quality of life that government of India is much concerned about. Across the rural and urban populace, ease of living essentially refers to (a) infrastructure connectivity (b) availability of basic amenities like electricity, water, sanitation etc. at the household level; (c) ability of the citizen to avail Government services remotely (d) availability of adequate livelihood opportunities. While the ease of doing business allows a profitable industry base to create job opportunities. Digital governance could transform both by strengthening the interface where the path of ease of doing business leads to ease of living while ensuring that the business world compliances and people life event based services are delivered without transactional friction.

To translate the vision of Atmanirbhar Bharat into reality, it is critical to create the right base and restructure the regulatory environment for businesses and citizens alike. Introducing the next generation of reforms relating to reduction in compliance burden in the country is a step in this direction. In the past, uncertainty and lack of clarity in regulations have been highlighted as the key impediments for growth in India and the central ministries with the support of states/union territories (UTs) are working on reforming regulatory regime with a great sense of urgency

***At the heart of the transformation is 'Ease of Living'***.

A multi-pronged strategy to have a transformative and multiplier effect to leapfrog to the next level of governance excellence along with improved Ease of Living (EoL) and Ease of Doing Business (EoDB), initiatives must be structured and implemented within limited duration. A customer-centric Government-to-Citizen (G2C) interface must be at the helm of the efforts made by the government. Industry must also partner with the government to tackle the most important issues impacting the industry's performance including time and cost spent to remain compliant with laws/regulations. The government's a four-pronged strategy, including simplification of compliances through self-certification and deemed approvals; elimination of compliance burden, wherever possible; transparency through digitisation i.e., creation of online interfaces and decriminalisation of laws with minor offenses, will help reduce regulatory cholesterol significantly

The next generation of reforms are expected to focus on reconsidering the 'purpose of compliances' and providing seamless end-to-end service delivery to citizens. These reforms will need to have digital backbone for making governance efficient and requiring much less human interrence.

In the last seven years, several such measures have been undertaken due to which there is an improvement in competitiveness, cost of doing business, innovation, and EoDB in India.

o Regulatory Compliance Portal: To eliminate/reduce compliances that have an adverse impact on time and cost of businesses, the Central government launched the portal, which acts as a bridge between industry and government agencies.

o Cost of doing business: There have been increased efforts towards identifying reform areas that reduce the overall cost of doing business. Sector-wise consultations are underway to measure the pain points regarding compliance cost, especially time and cost required for preparation and fees paid to intermediaries to remain compliant with the current rules.

o PM GatiShakti: This initiative is expected to enable better communication between the public and the business community regarding upcoming connectivity projects, business hubs, industrial areas and surrounding environment.

o One Nation One Ration Card (ONORC): Department of Food and Public Distribution has launched 'Mera Ration' App to facilitate One Nation One Ration Card (ONORC) scheme. The initiative enables 69 crore National Food Security Act (NFSA) beneficiaries, covered under the scheme, to locate the nearest

fair price shop, verify details about their food grain entitlement and manage transactions across the nation.

***Citizen-centric approach for key inclusion in the transformation plan***

The agenda for the next phase of reforms for reducing the compliance burden has EoL at its core. During the National Workshop on Reducing Compliance Burden in December 2021, the Central government envisioned a holistic approach to:

- o Consolidate and revamp the existing digital infrastructure by building a National Single Sign-On (SSO) for Citizens (a one stop for all government services)
- o Build an effective grievance redressal mechanism with increased accountability
- o Break the silos between its departments which will help in reducing the duplicate compliance requirements as well as overall cost to business.

Various government agencies at both the central and state levels have built multiple interfaces for providing citizen services. These interfaces currently have different levels of usability, comprehensiveness, security, and privacy. The multiple applications led to several pain points for citizens, including the requirement of multiple login credentials, the need to prove identity for every new application and the lack of a mechanism for identifying entitlements for citizens. Thus, to enhance easy and quick access to citizen services, the government is planning to converge most of these services into India's first citizen-centric portal with 'National Single Sign-On' and welfare benefits delivery for all citizens.

The public grievance redressal mechanism of India operates somewhat on a decentralised basis. Despite having multiple mechanisms for citizens, the quality and effectiveness of grievance redressal as well as the timeliness remain the major challenges. With the advent of new-generation technologies such as bots and Artificial Intelligence (AI), it is the right time to make the grievance redressal mechanism more robust and effective. It is recommended that a dedicated accountability-based mechanism shall be established for percolation of the impact at grass root level i.e., local bodies, Gram Panchayats, etc.

In conclusion, recent efforts have brought dividends already towards EoDB as the country ascended 17 notches, ranked at 63rd position in the Ease of Doing Business report 2020 published by The World Bank. The mood in the industry and businesses is buoyant noticing the willingness displayed by the government to take all stakeholders on-board. The mindset is evolving from 'not able to understand complexities' to 'it is so simple to start a business.'

The objective of digital governance is to achieve a progression from "digitisation", through "e-government" to "Digital Government". New approaches are needed to support a shift from government-centred services, through a focus on citizen-centred approaches, and on to environments in which citizens and businesses determine their own needs and address them in partnership with governments, which are supported by new governance frameworks. The challenge is not to introduce digital technologies into public administrations (digitisation); it is more transformative: to integrate the use of digital technologies into public sector modernisation efforts (Digital Government).

Digital Governance will therefore play a key role to leverage this transformation of the public sector at large, given its potential to increase productivity and inclusiveness of service production and delivery in public welfare areas. In the short term, it will be a precondition for establishing and maintaining sound Ease of Doing policies and Ease of living; in the longer run, it will be equally important to maintain public sector's credibility in terms of efficient and effective delivery of high-quality services that are shaped by and responsive to users' needs, thus nurturing public trust in governments' capacity to boost more inclusive processes and growth.


Department of Administrative
Reforms and Public Grievances