

Critique of Legal Framework Regulating E-Governance in India

Dr. Ruchi Lal

Assistant Professor-II, Amity Law School, Amity University, Noida, U.P. (India)

ARTICLE DETAILS

Article History

Published Online: 10 February 2019

Keywords

Information and Communication Technology, E-Governance, Legal & Regulatory Framework

*Corresponding Author

Email: lal.ruchi1[at]gmail.com

ABSTRACT

An imperative investment for economies across the world today, especially for developing countries like India, is e-governance with a vision of ensuring effectiveness and transparency in governance. At the outset, the focus of e-governance outlay was primarily on strengthening the hardware aspect of Information and Communication Technology hardware. However, the second generation expenditure now is more focused upon making e-governance a driving force for creating SMART governance wherein SMART stands for simple, moral, accountable, responsive and transparent governance. In India as well, the focus of e-governance is to realise the vision of digital India i.e. to ensure that governmental services are made available to public at large via electronic media. This paper begins with tracing the development of ICT in India and highlights the need for having a holistic statutory backing for E-Governance in the country. The paper further progresses to scrutinize the present legal & regulatory framework addressing e-governance initiatives. The paper ends with the argument that there is an inadequate legal framework in India to regulate e-governance since these existing legislations do not address all aspects of e-governance, such as e-procurement, data protection, privacy policies and re-use of information. Moreover, the absence of legal framework in the country that mandates that general public, businesses and other institutions can claim e-governance as a matter of right. Therefore, the paper proposes that there is need for new legislation that comprehensively deals with all legal aspects associated with effective delivery of e-governance services in the country like cyber security, privacy protection, data safety and protection thereof etc.

"E-Governance is easy governance, effective governance and economical governance."

-Shri Narendra Modi¹

1. Introduction

Today Information and Communication Technology (ICT) has become a crucial facet of all human activities. Its use whether in the mode of internet, personal computer, and mobile phone has completely transformed the manner in which people network with each other and government institutions transact business and avail public services. Amongst its many applications, perhaps the most arduous use of ICT is e-governance.²

E-governance is, in essence, the use of ICT for the purpose of making government services accessible to all, transmission of information, integration of various sectors and services between government and citizens, government and employees, government and business enterprises, and Government to government.³ The overall aim of e-governance is to establish 'Simple, Moral, Accountable, Responsive and Transparent (SMART) governance.'⁴

Dr. APJ Abdul Kalam, has conceptualised e-governance as a transparent tool which has continuous access, is secured and ensures authentic transmission of data interjecting departmental obstacles, thus providing a just, fair, reasonable and impartial services to the citizen of the country.⁵

In India, electronics was brought into focus with the establishment of Department of Electronics in 1970 followed by setting up of National Informatics Centre in 1977.⁶ However, first crucial step towards realising e-governance was taken by the Indian Government with the launching of the national satellite-based computer network i.e. NICNET in the year 1987. Thereafter, progress in this regard was made with the establishment of the District Information System programme primarily aimed at computerizing all district offices across the country. During that phase, few of the government's e-governance projects included railway computerization, land record computerization, etc. which primarily laid emphasis on the expansion of information systems.⁷

Although these initiatives were directed towards delivering electronic services to the public, they failed to achieve desired result because of the limited features. The inaccessible and

¹ PM of India

² Sumanjeet, E-Governance: An Overview in The Indian Context. The Indian Journal of Political Science 2006; 64: 4: 859.

³ Sharma K S, Rathore Vijay Singh and Jawaria K.L. E-Governance in India - Trends, Prospects, Challenges and Solutions. 2016; 3:2348.

⁴ Yadav Kiran and Tiwari, Sanatan. E-Governance in India: Opportunities and Challenges. International Journal of Advance in Electronic and Electric Engineering. 2014; 4:6, 675.

⁵ Inaugural address at IIT Delhi during International conference on e-Governance, 18th December, 2003.

⁶ Implementing e-Governance Reforms, December 8, 2008. available at http://arc.gov.in/11threp/ARC_11thReport_Ch6.pdf. [accessed on 15 August, 201].

⁷ Digital India: Power to empower, (January 4, 2017). available at <http://www.digitalindia.gov.in/content/introduction>. [accessed on July 30, 2018].

less interactive systems exposed major fissure that were upsetting the full-fledged adoption of e-governance. This scenario brought to the forefront the necessity of comprehensive planning and implementation of requisite infrastructure for making e-governance initiative a thriving success in the country.

2. National e-Governance Plan

In order to realize the vision of digital India, in the year 2006, National e-Governance Plan (NeGP) was floated with the vision “to make all government services available to the citizens of India via electronic media”. In all there were thirty one Mission Mode Projects(MMPs)under NeGP encompassing within its ambit diverse areas like covering a wide range areas like cultivation, revenue records, health, education, passports, land records, commercial taxes etc. To a large extent MMPs have been implemented, executed and started rendering complete or partial range of envisaged services. Apart from this, the Indian government, keeping in mind the mission of transforming e-Governance for making governance effective and keeping in perspective the necessity to employ advanced technologies like Cloud computing and smart phones, the Government has planned to enforce “e-Kranti : National e-Governance Plan (NeGP) 2.0” under the Digital India programme.

3. Need for Statutory Backing for E-Governance

E- Governance employs information technology for the delivery of e- governance services. There arise numerous legal issues so far as use of information technology in the government sector is concerned like legality of electronic transactions, electronic records and contracts, data protection and security etc. All these dimensions should be adequately addressed within the country's legal framework, so as to ensure legal sanctity to the entire e –governance initiative. Furthermore, e-governance represents new form of governance, which is dynamic, and exponential. It needs dynamic laws, keeping pace with the technological advancements. But this new dispensation of e-governance requires new set of laws to redefine the old structure of governance by meshing with the new structure of the web.⁸

Physical Governance v. E-Governance⁹

Physical Governance	E-Governance
Statutory recognition to physical documents	Statutory recognition to electronic records
Signatures	Digital and Electronic signatures
Publication of Official Gazette	Publication of Electronic Gazette

Additionally, the scope of NeGP is quite vast covering within its ambit almost all the dimensions of e- governance ranging from delivery of government services to business process re-engineering,¹⁰ therefore, it is imperative that NeGP

⁸Sharma Vakul. Information Technology: Law and Practice. 3d ed., Universal Law Publishing, New Delhi.2013:48.

⁹ Id 49

¹⁰Samtani Anil and Harry SK Tan. Regulatory and Policy Issues of E-Commerce in Asia. International Journal of Law and Policy Issues. 2004; 63.

is regulated, supervised and implemented within a strong legal framework.

4. Legal & Regulatory Framework in India

Although the legal system in India is dynamic and robust backed by an activist judiciary, yet it is unable to keep pace with the growth and development of advancing technologies. As of now there is absence of all-inclusive and enabling legal framework that can regulate and ensure mandatory e-governance services in India. However, despite the lack of any specific legal framework, there are several laws the provisions of which can be used to regulate e-governance. The constituents of the current statutory and regulatory framework in India for addressing e- governance initiatives are:

A. The Information Technology Act, 2000 ((IT, Act 2000))

IT, Act 2000, based on the model framework provided by United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, came into force on October 17th, 2000 There are 94 sections in the Act which are categorised into thirteen Chapters and four Schedules.

Aims and Objectives - IT Act, 2000¹¹

1. To give legal recognition to transactions executed through electronic means.
2. To confer legal sanctity upon digital signatures and also to provide regulatory regime for the same.
3. To enable e- filing of documents and e-payments.
4. To enable e-governance and to boost the usage of electronic records and digital signatures in public sector.
5. To prevent computer crimes and to put in place a deterrence mechanism in the form of civil and criminal liabilities in case of violation of the Act
6. To make consequential amendments in the Indian Penal Code, Indian Evidence Act, 1872, and the Reserve Bank of India Act, 1934.

Major Components of IT Act on E-Governance

Chapter III of the Act deals with e-governance. Some important provisions in this regard are:

i. Statutory recognition of e- records:

Sec. 4 of the IT Act brings forth the basic premise of IT Act, 2000 that the medium in which a record is created or retained does not affect its legal significance because the substantive law governing the transaction may require non-electronic records or signatures. Therefore, the said section, in effect, overrules the substantive laws on these requirements.¹²

ii. Statutory recognition of e-signatures¹³:

Sec. 5 of the Act provides for statutory recognition of e-signatures. Following conditions are required to be fulfilled for the section to be applied:

¹¹PawanDuggal, “Cyber Law – An Overview”. available at <http://www.cyberlawindia.com>. [accessed on 17 August, 2018].

¹²Gupta, Apar. Commentary on Information Technology Act. 2ndedn, Lexis Nexis, New Delhi. 2016:75.

¹³Substituted by the Information Technology (Amendment) Act, 2008, Section 2 for ‘digital signatures’.

- a. The concerned legislation should make it mandatory that the document in question should be signed by the person;
- b. an e- signature is placed in lieu of such signature; and
- c. such signature is appended in the form given by the government.

By the IT (Amendment) Act, 2008, Section 5 now adopts technology neutrality by recognising electronic signatures in place of digital signatures and hence, moves away from its earlier technology specific approach.

This section places e- signatures on the same page as handwritten signatures so far as authenticating any electronic record is concerned.

iii. Use of Electronic Records (e-records) and Digital Signatures in Government and its Agencies

The Act contains provision for the use of e- records in government service delivery. In this regard Sec. 6(1) of the Act is relevant which provides that where any law requires that filling of any document etc., or issue of any licence, sanction or approval; or receipt or payment of money by a government department has to be in a particular manner, the said prerequisite shall be considered to have been fulfilled, if such filing, receipt etc. has been done in the electronic form.

The above prerequisite shall be considered to have been fulfilled, if such filing, receipt etc. has been done in the electronic form, is effected by means of such electronic form as may be determined by the government.

The sweep of sub-section (1) is very vast. It recognises e-filing of documents, issue of online certificates or licenses and the receipt of money via electronic means or e-Payments.¹⁴This provision is intended to apply to all governmental activities with the approach to execute e-governance for every 'government to citizen' as well as 'government to business' interactions.¹⁵

Electronic Filing

Section 6(1) (a) of the IT Act, provides for "filing of any form, application or any other document", electronically. Since the electronic filing revolves around the usage of internet and appropriate software to permit documents to be used by the government and because the documents are transferred online, the method is called 'e-filing'.¹⁶ The concept has many benefits like riddance of expenses involved in delivery by hand, elimination of physical storage costs, and quick retrieval of e-documents by public authorities amongst others.

Electronic Grants

Section 6 (1) (b) of the IT Act, provides, award of any licence, permit, sanction or approval, by electronic process. The Government has implemented a comprehensive system for e- procurement via website "www.eprocurement.gov"

through which it provides e-Tendering services. It serves as a platform for its members to have access to the online tenders issued by several government departments.¹⁷ The website incorporates all the relevant areas like purchasing, connects buyers and suppliers through electronic exchange of tenders, catalogues, contracts, invoices etc.¹⁸

Electronic money transfer

Section 6 (1) (c) of the IT Act, provides for, "receipt or remittance of money in an electronic form". The introduction of electronic payment system into government activities may result in more effective use of public funds. For private parties, e- payment opens up enormous opportunities for efficient financial services and commerce.

Provisions for the usage of e-records and digital signatures

Section 6(2) requires the government to frame guidelines for the form in which e- records shall be filed, created or issued; and also lay to lay down the rules as to the mode of the remittance of any charges for the for filling, creation or issue such e- records.

In pursuant to the above section, the Information Technology (Use of Electronic Records and Digital Signatures)Rules, 2004 has been enacted by the Government which lays down essentials for filing of form, application or any other document; issue any licence, permit, etc.; and remittance of any fees.

iv. Holding of e-records

Section 7 of the IT Act, 2000 enumerates rules regarding the holding of e-records. It provides that if a specific legislations demands that documents or information should be kept for a specific duration, then the condition shall be presumed to be fulfilled if such document or information is stored in soft copy provided:

- The data incorporated therein is available for future reference;
- The e-record is stored in the form in which it was initially generated, forwarded or received,
- The particulars which will aid in search of the origin, destination, etc. such e-record is available in the electronic record.

However, the above provision will not apply "to any data which is robotically generated exclusively with the objective of aiding an e- record to be dispatched or received".¹⁹

The rules contained in Section 7(1) pertain to the retention of records that are originally in e- form and to other physical documents that have been converted to electronic records.²⁰Furthermore, the reading of the said section makes it clear that it does not stipulate any specific period for the

¹⁴Reading Material for E-Governance Training Sessions.YashwantraoChavan Academy of Development Administration, Pune. 116.

¹⁵ Supra note 8 at 51

¹⁶Supra note 12 at 81

¹⁷Government of India, Tender Management Services,(January 4, 2017).available at <https://tender.eprocurement.gov.in>. [accessed on 15 April,2018].

¹⁸ Ibid.

¹⁹Proviso to Section 7 (1) of the IT Act, 2000.

²⁰ Supra note 12 at 93.

holding of records but prescribes minimum standards to be applied thereof. These minimum standards are:²¹

- a. *Accessibility*: The records must be accessible for subsequent use.
- b. *Format integrity*: The electronic record must be held up in the form in which it was formerly stored because any change in the format can alter material characteristics of the record. With this aspect in mind, Section 7 (1) provides that, even if there is a change in format, the electronic record shall be "in the format which can be demonstrated to represent accurately the information originally generated, sent or received."
- c. *Identification*: It is essential that any electronic record can be searched easily and therefore, any record should be retained in the format which would facilitate discerning of origin, destination, etc. of such records. Section 7(2) provides that, "nothing in this provision shall be applicable to any regulation that specifically demands for the holding up of documents or information in the form of e-records." Additionally, this section also provides that standards incorporated in this are merely minimum standards and it does not preclude the government authority from putting in place additional requirements for retention of records.

v. Publication of rules, regulations etc. in electronic gazette

The IT Act, under Sec.8 incorporates provision for e-publication of any rule, regulation, order, bye-law etc. in an electronic gazette. This section equates electronic gazette at par with official gazette.

Voluntary implementation of E-governance

Section 9 of the Act provides that Sec. 6, 7 and 8 of the Act are to be implemented voluntarily by Central or State Government or by any body or authority established thereof.

Thus, Section 9 does not confer justiciable e-governance rights as it does not allow any person to demand the concerned Central or State government department to retain any document in e-format.

The *raison d'être* behind this section is perhaps that those governmental agencies who are not yet logistically empowered to adopt ICT are not unreasonably compelled to do so. Additionally, it is also required to be noted that conversion of physical documents into electronic record is rather a tedious process.²² Nonetheless, the point of argument is whether the Central Government should fix a time frame within which e-governance should be implemented mandatorily and whether section 9 merely permits administrative lassitude.²³

vi. Power of Government to frame rules for e-signatures

Section 10 of the IT Act gives Central Government the authority to frame rules so as to prescribe, "(a) the category of e- signature; (b) the mode and layout in which e- signature should be attached; (c) the mode or method which assists in recognition of the individual appending the e- signature; (d)

²¹ Supra note 12 at 93.

²² Supra note 12 at 97.

²³ Ibid.

regulate the mechanism to integrity, security and confidentiality of e- records; and (e) any other ancillary issue which is imperative to be dealt with in order to provide legal effect to e-signatures."

B. IT (Amendment) Act, 2008

The IT Act, 2000 was amended in the year 2008 in order to include certain additional provisions, and to alter certain provisions. With regard to e-governance following changes were introduced:

i. Delivery of services by service provider

Delivery of government services by the use of IT would be more effective when delivered through the cooperation of private sector. Hence, for allowing private sector into the domain of delivery of e-government services, and giving a legal mandate to Public Private Partnership, it was felt that there was a need for legislative sanction in this regard. This need had been given shape in the form of Section 6A (1) which stipulates that for effective delivery of services through electronic means to the general public, the government may appoint a private service provider.

Furthermore under Section 6A (2), the government has the authority to provide incentives to private sector provider by permitting them to directly collect money for providing services. The charges contemplated here are not to be determined by the service providers itself but by the government which shall notify them in the rules.²⁴

ii. Audit of documents etc. kept in e- form

Since increasingly documents and records are being stored in electronic form, it has become imperative to audit such records. In this regard, Section 7A through the IT (Amendment Act), 2008 was inserted. Sec.7A of the Act stipulates that where a provision of a law is asking for the audit of documents, then it shall also include an audit of the documents which are processed and maintained electronically. Here an audit may be defined as an examination of records to determine the genuineness of the data in records.²⁵

iii. Validity of contracts formed through electronic means

Under the IT Act of the year 2000, there was absence of any specific provision pertaining to e-contract; however, Amendment Act of 2008 has inserted section 10A which provides legitimacy to contracts executed electronically.

Section 10A applies when the several stages of contract formation, such as the offer, acceptance, revocation thereof is done electronically. The provision states that such a contract will not be termed invalid merely because these steps of contract formation were concluded online.

C. The Right to Information Act, 2005 (RTI Act, 2005)

The RTI Act, 2005 is the country's foremost legislation that imposes an obligation upon the government to adopt e-governance. Main objective of the Act is to bring about transparency in the functioning of the government agencies and is based on the premise that all information pertaining to

²⁴ Section 6(4) of Information Technology Act, 2000.

²⁵ Supra note 12 at 97.

the government and its agencies belongs to the people of the country. Section 4(1) of RTI Act specifies that all the authorities of the government have to keep its records in such a manner that it facilitates access to information under the Act, and also to ensure that all the said records are computerised within reasonable time frame and are made available through network all over the country. Also Sec. 4 (2) of the Act requires the public authorities to take efforts to make available to the general public as much information as possible at regular intervals so to minimise the use of Act by the public.

E-governance can never be a successful endeavour till RTI Act is fully implemented. Also it is a fact that the success of RTI is directly dependent upon full-fledged computerisation of public records.²⁶ Digitisation of all government documents is important for the reason that it will address the information needs of citizens by giving prompt access to the services of the government, an objective which the RTI Act vehemently promotes.²⁷

D. Cyber Crime Provisions in IT Act, 2000 and IT (Amendment) Act, 2008

In common parlance cyber-crime is understood as any unlawful act where computer is used as a means or is targeted or can be both. Since e- governance primarily involves the use of ICT, therefore, for effective monitoring, implementation and delivery of any e-governance service, it becomes imperative for the government personnel and operators involved to have knowledge about cyber crime provisions and legal implications of the violations thereof. Summary of cyber crime provisions in IT Act are given below:

a. *Punitive action for damage to computer, computer system, etc.*

Section 43 identifies ten different wrongs of causing damage to the computer, computer system or computer network.²⁸

²⁶HabibullahWajahat, "Using Right to Information to its fullest capacity is challenging", Dataquest, [2004] and Habibullah, Wajahat, "RTI and E-Governance Are Twins, and Are Inseparable", April 11, 2008, available at <http://www.dqindia.com/rti-and-e-governance-are-twins-and-are-inseparable/> [accessed on August 1, 2018].

²⁷Abhishek Jain AndAarushiJainpromoting, "Right To Information Through E-Governance – A Case Of E-Soochna And Other Initiatives", August 2, 2011. available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1903798 [accessed September 1, 2018].

²⁸ Section 43 of the IT Act, 2000: [Penalty and compensation] for damage to computer, computer system, etc. -If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,-

(a) accesses or secures access to such computer, computer system or computer network [or computer resource];

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

Section 43A was added by the IT (Amendment) Act with the objective of protecting personal data and privacy. It makes it mandatory for "body corporate" handling sensitive personal data (e.g. mail services, banks, insurance companies) to incorporate reasonable security mechanisms as specified by the government. In fact, the present section prescribed a redressal mechanism whereby, any affected person who has suffered loss can seek compensation from a body corporate that has been careless in effecting reasonable security practices.

b. Tampering with Source Code

Computer source code is the intellectual property invested in the computer programmes and Sec. 65 of the IT Act is intended to prevent the tampering of the computer source documents. According to Section 65 if any person deliberately hides, destroys or modifies computer source code, when such computer source code is required to be kept by law, he shall be punished with fine up to Rs.2 lakh and / or imprisonment which may extend up to three years.

c. Computer Related Offences

Under Section 66, if any person, in bad faith, does an act which is specifically mentioned in Section 43, he is liable to punished with imprisonment which may extend up to three years or with fine up to Rs. 5 lakh or both.²⁹

d. Other Computer related offences:

- 66A: Sending offensive Messages - relates to information that is manifestly offensive or menacing or false information, including Cyber Stalking and Phishing.
- Section 66B: Receiving a Stolen Computer Resource
- Section 66C: Identity Theft –
- Section 66D: Cheating by impersonation - applies to Phishing, Job Frauds etc
- Section 66E: Violation of Privacy - applies to Video Voyeurism
- Section 66F: Defines Cyber Terrorism and punishment for the same.
- Section 66F (A): Act done with the intention to harm the unity, integrity, security or sovereignty of the country.

E. Indian Penal Code

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;]

[(j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;] 48 [he shall be liable to pay damages by way of compensation to the person so affected]."

²⁹Supra note section 43

Apart from IT Act, 2000 and amendment of 2008, some of the cybercrimes are also covered by Indian Penal Code. A brief summary of the concerned provisions is given below:

Cyber Crimes under IPC

IPC Section	Cyber Crimes
Sec 503	Sending intimidating-mails
Sec 499, 500	Sending defamatory mails
Sec 463, 470, 471	Forgery of electronic records
Sec 420	Bogus websites, cyber frauds
Sec 416, 417, 463	Email spoofing
Sec. 383	Web - Jacking
Sec 405, 406, 408, 409	Criminal breach of trust / Fraud
Sec 204, 477	Destruction of electronic evidence
Sec.193	False electronic evidence
Sec.167,172,173,175	Offences by or against public officials

areas associated with effective delivery e-governance services that have largely been left unaddressed by these legislations. Additionally, there is absence of legal framework in the country that mandates that general public, businesses and other institutions can claim e-governance as a matter of right. Therefore, there is need for new legislation that comprehensively covers all the legal aspects pertaining to effective delivery of e-governance services in the country. This legislation must contain provisions for effective regulation of e-governance but at the same time, should not be over regulative so as to that smother the growth of technology.

F. Indian Evidence Act (IEA),1872

IEA was amended to take cognizance of electronic evidence, via second Schedule of IT Act of the year 2000 and Part IV of IT Amendment Act, 2008:

- i. Section 3 of the IEA amended to take care of admissibility of Electronic Records as evidence along with the physical records as part of the documents which can be produced before the court for inspection.
- ii. Section 47A of the IEA makes expert opinion of certifying authority as to digital signature of an individual a relevant fact.
- iii. Section 67B: Conditions to be fulfilled for admissibility of electronic records as evidence
- iv. Section 73A: The verification of Digital Signature should either be by Controller of CAs or by any other person using the signer's public key

5. Conclusion

For enhancing technical integration across the country and in a bid to advance e-governance implementation, the Modi government is proactively working towards Digital India initiative the proposed target for completion of which is set for 2019.³⁰ Amongst the primary challenges which Digital India initiative will face will be lack of legal framework, absence of privacy and data protection laws, insecure Indian cyberspace amongst others.

Although the IT (Amendment) Act, 2008, IPC and RTI, 2005 contains provisions for regulating e-governance services, however, aforesaid deliberations on these statutes makes it apparent that there is absence of appropriate legislation to regulate e-governance since these legislations do not address all aspects of e-governance, nor would it be reasonably expected to. Areas such as e-procurement, data protection, privacy policies and re-use of information are some of the

³⁰Digital India is an initiative of Government of India to integrate the government departments and the people of India. It aims at ensuring the government services are made available to citizens electronically by reducing paperwork. The initiative also includes plan to connect rural areas with high-speed internet networks. Digital India has three core components. These include creation of digital infrastructure, delivering services digitally and digital literacy.