The corporate world is witnessing various changes. Corporate world’s networks are increasingly being targeted by cyber criminals. Each passing day comes up with some news about breaches on corporate networks at global and Indian levels. For running the day-to-day affairs of corporates, the electronic format is the defacto format.

Corporates are being assisted in their compliances under the Indian laws by Company Secretaries. Hence, Company Secretaries become essential catalysts in enabling companies to ensure their compliances with the law.

However, Company Secretaries need to be mindful of the fact that increasingly all their activities are coming under the umbrella of not just sector specific legislations but also of the Indian mother legislation to deal with data and information in the electronic format being the Indian Information Technology Act, 2000. In that sense, the Indian cyber law assumes significance.

At this juncture, it is relevant for us to understand what the IT Act, 2000 offers and its various perspectives.

The object of the Information Technology Act, 2000 as defined therein is as under:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

Towards this end, the said Act thereafter stipulates numerous provisions. The said Act aims to provide for the legal framework so that the legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The said Act further states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The said Act purports to facilitate electronic intercourse in trade and commerce, eliminate barriers and obstacles coming in the way of electronic commerce resulting from the glorious uncertainties relating to writing and signature requirements over the Internet. The Act also aims to fulfil its objects of promoting and developing the legal and business infrastructure necessary to implement electronic commerce.

Chapter-II of the said Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person by the use of a public key of the subscriber can verify the electronic record.

---

1 Authored by: - Pavan Duggal, Advocate, Supreme Court Of India
This fact is of the particular relevance that the Indian Information Technology Act, 2000 has provided the legal framework for electronic authentication. Not only digital signatures have been granted legalities but more significantly by virtue of the Information Technology (Amendment) Act, 2008, the concept of electronic signature has been introduced in the law. The term “electronic signature” has been defined in very broad term to mean authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes Digital Signature. At present Company Secretaries are increasingly using digital signatures for variety of electronic and digital purposes. They need to be mindful of the legal nuances and ramifications of the said electronic authentication.

Chapter III of the Act details about Electronic Governance and provides interalia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

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

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

The said chapter also details about the legal recognition of Digital Signatures. The various provisions further elaborate on the use of Electronic Records and Digital Signatures in Government Agencies. The Act further talks of publications of rules and regulations in the Electronic Gazette.

Chapter IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities and also specifying the various forms and content of Digital Signature Certificates. The Act also provides for the need for recognising foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

Chapter VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

Chapter IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer system etc. have been fixed as damages by way of compensation not exceeding Rs. 500,00,000/- to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said act or rules framed thereunder. The said Adjudicating Officer has been given the powers of a Civil Court.

There is a provision in Chapter X which envisage the Cyber Appellate Tribunal shall be an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred. The said Tribunal shall not be bound by the principles of the Code of Civil Procedure but shall follow the principles of natural justice and shall have the same powers as those are vested in a Civil Court. Against an order or decision of the Cyber Appellate Tribunal, an appeal shall lie to the High Court.
Chapter XI of the said Act talks about various offences and the said offences shall be
investigated only by a Police Officer not below the rank of an Inspector. These offences
include tampering with computer source documents, publishing of information which is
obscene in electronic form, breach of confidentiality and privacy, misrepresentation,
publishing Digital Signature Certificate false in certain particulars and publication for
fraudulent purposes.

The said Act also provides for the constitution of the Cyber Regulations Advisory Committee
which shall advice the government as regards any rules or for any other purpose connected
with the said act. The said Act also has four Schedules which amend the Indian Penal Code,
1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve
Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

Various new provisions have been added in the Indian cyber law by virtue of the Information
Technology (Amendment) Act, 2008, which have impact upon the day to day functioning of
corporates in India.

In addition, the increased attacks on corporate networks bring in forefront the issue of
protection and preservation of cyber security of corporate networks.

In fact, data protection and privacy are concepts which are intrinsically linked with each other
and have a direct connection to each other. However, both the said concepts are looking at
different objectives and ends. Consequently, data protection and privacy are distinct concept
which are sought to be addressed by distinct legal frameworks in different parts of the world.

In the Indian context, we quickly need to appreciate that India does not have either a
dedicated data protection law or a dedicated law on privacy. India has adopted the hybrid
approach of coming up with one mother legislation that deals with all aspects pertaining to
the digital format.

Following the adoption of the UNCITRAL Model Law on Electronic Commerce by the
General Assembly of the United Nations, India started working on its own national
legislation to promote e-commerce. Consequently, the Information Technology Act, 2000
was enacted for the purposes of giving a boost to e-commerce and providing a legal
framework for electronic governance activities. By the time the law got to be amended by the
Information Technology (Amendment) Act, 2008, the law transformed itself from being a
mere e-commerce enabling legislation to becoming an all comprehensive mother legislation
dealing with all aspects pertaining to use of computers, computer systems, computer
networks, computer resources and communication devices as also data and information in the
electronic form. Under the said legislation, some provisions have been incorporated which
have an impact upon protecting data. The Government of India has been given the power to
come up with various rules and regulations to give effect to the various provisions of the
Information Technology Act, 2000. Consequently, in April 2011, the Government of India
came up with four set of rules which are collectively known as the Information Technology
Rules, 2011. The said Rules have sought to create a distinctive legal framework for data
protection in India. Of further relevance in the said Rules are two rules being the Information
Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or
Information) Rules, 2011 and the Information Technology (Intermediaries Guidelines) Rules,
2011.
Seen from another perspective, the said Rules have gone ahead and provided for various provisions for data protection and go much beyond the scope and ambit of the mother legislation, being the Information Technology Act, 2000. In that sense, the said Rules have over reached the ambit and scope of the main legislation being the Indian cyber law and have instead come up with a surrogate regime on data protection. By virtue of the landmark judgment of the Supreme Court in the case of Shreya Singhal v/s Union of India, the constitutional validity of the various provisions of the Information Technology Act, 2000 as also the Information Technology (Intermediaries Guidelines) Rules, 2011 were upheld.

From the corporate angle, it needs to be appreciated that the Information Technology Act, 2000 and also the rules and regulations made thereunder are the relevant mother code that needs to be complied with by corporates in India till such time; the said legislation is not amended, altered, reviewed or modified accordingly.

A Body corporate, which receives, possesses, deals or handles information in India is mandated to have various policies and compliances in place.

Corporates need to be alive to the fact that the law has gone ahead and given an expansive definition of personal information to mean any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. Further, the law has gone ahead and defined what constitutes sensitive personal data or information.

Sensitive personal data or information of a person has been defined to mean such personal information which consists of information relating to;—

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vi) biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

Companies are required to have detailed terms and conditions, rules and regulations as also privacy policies, while handling or dealing with information including sensitive personal information or data. Companies should also have policies for collection, preservation, retention, disclosure and transfer of sensitive personal information.
Further, the Indian cyber law recognizes all corporate which deal with personal information and sensitive personal data of others as intermediaries. The said intermediaries are mandated to exercise due diligence while discharging their obligations as intermediaries under the Information Technology Act, 2000. Consequently, in this context the said companies are mandated to have in place reasonable security practices and procedures as also comprehensive documented information security programs and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with information assets being protected with the nature of the business.

Further, if the said corporates are dealing, handling or processing sensitive personal data or information, they have no choice but to implement and maintain reasonable security practices and procedures. If they fail to do so, and pursuant to their failure and negligence to implement and maintain reasonable security practices and procedures, there is a wrongful loss or wrongful gain caused to any person, the same becomes a ground for seeking unlimited damages by way of compensation against the said corporates. Further, the failure to comply with the mandatory requirements of law, could also expose the top management of the companies to criminal liability in the form of imprisonment and fine.

Thus, corporates in India increasingly need to ensure that their compliances under the Indian cyber law are in place.

As of date, the law pertaining to electronic data and its protection is only beginning to evolve. In actual terms, the Indian cyber law and rules and regulations made thereunder concerning data protection are being complied in breach rather than in the observance. However, corporates have to quickly realize that there are immense reputational risks for not complying with the law. Corporates have to ensure that they have documented compliances with the law in order to protect themselves from any unforeseen exigency that could land at their doors unannounced. Further, in the context of privacy, the law does not talk much about privacy. The Indian cyber law has adopted a somewhat primitive approach on personal privacy. Issues of data privacy have not been elaborated in detail. There has been some talk for coming up with a dedicated law on privacy in the country. However, that has not seen much light of the day. Justice AP Shah Committee recommended to the Government, various steps that need to be taken for ensuring privacy. However, the said recommendations currently have not been implemented.

Seen from an overall perspective, companies today have to realize that they are not just intermediaries but also data repositories in the sense that they are dealing with huge volumes of data of employees, business partners, associates and also third parties. In such scenario, companies as intermediaries must ensure compliance with the law in order to be on the right side of the law. Failure to comply with law, could expose the company to unnecessary civil and criminal consequences. It should be the top most priority of any company to protect the data privacy of the individuals along with securing its top management and their legal interests.

It is in this context that the role of professionals like Company Secretaries becomes increasingly significant in today’s time. The onus is on the Company Secretaries to ensure that they themselves are aware about the nuances pertaining to electronic authentication and other issues impacted by Indian cyber law and then appropriately advise their clients to be on the right side of the law.
Compliance with the existing law, however deficient or inadequate, is the only way going forward for corporates for the purposes of protecting and preserving their legal interests.

*****