08 November, 2019

POLICYINSIGHTS

INSTITUTE OF POLICY STUDIES OF SRI LANKA

PRIVACY AND DATA PROTECTION IN THE 4IR

From the IPS flagship publication 'Sri Lanka: State of the Economy 2019'

Each day, a vast amount of information is transmitted, stored, and collected across the globe, enabled by the rise of computing and communication power. Technologies and innovation have increased the need for privacy regulation, whilst requiring existing privacy regulations to adapt to these new advancements. The emergence of cloud computing, the internet of things (IoT), 5G networks and big data analytics present new challenges to the field of data protection and privacy.

Data protection has been placed high on the political agendas globally; In 2015, the United Nations appointed a special rapporteur on the right to privacy, the European Union (EU) ratified its new privacy legislation in 2016, data protection is now being included in many trade agreements and data protection has been a key concern in several high-profile court cases in relation to national surveillance issues.

The growing threat of cybercrime reinforces the need for adequate data protection and data privacy measures. In 2018 alone, cyberattacks, including those on systemically important industries like financial services have increased fivefold, and new estimates put the estimated global costs of cyberattacks at USD 8 trillion over the next five years. A large proportion of cyberattacks result in unauthorised access to sensitive data, including that of personal nature, in turn creating data privacy concerns. Some estimates suggest that several billion datasets are breached every year, with some attacks and data losses taking months to detect.

Why Data Protection is Necessary for Sri Lanka

Data protection is increasingly becoming more relevant to Sri Lanka with the rapid rise in digitalisation and digital connectivity. By early 2017, Sri Lanka had more active mobile phone subscriptions than people, with 124 subscriptions per 100 persons. As of 2017, over 75 per cent of the 6.2 million internet users in Sri Lanka were estimated to access the internet through smart phone devices. This continued rise in digitalisation generates more and more data, and heightens the requirement for data protection and privacy laws.

Within Sri Lanka, there is also an increasing reliance on digital and cloud services, all of which collect data. For example, transportation applications such as Uber and PickMe both collect data for offline analysis. In addition, there is an increased usage of social media platforms and cloud communication platforms for email and calendar management (e.g.

Global costs of cyberattacks at USD 8 trillion over the next five years

Google mail and Calendar). These systems, being the primary means of communication, collect large amounts of data daily and then target advertisements based on these collected data.

Furthermore, the use of Virtual Private Networks (VPN) also brings in privacy concerns. In certain cases, applications providing this VPN service for free, sell consumer internet activity data to advertisement targeting agencies. Given the fact that VPNs can capture all data that are being transmitted or received by a device, the amount of information captured can be very detailed (e.g. unencrypted

messaging services, location, contact information, app usage) and this information can easily be personally identifiable in nature.

As Sri Lanka is set to enable 5G transmission in 2020, the need for comprehensive privacy legislation is heightened. A large amount of data sent over current mobile networks is not encrypted or if it is, leverages outdated and easily by-passable encryption methods and are therefore susceptible to interception.

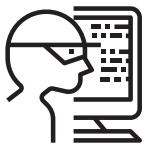
The need for cyber security and data protection becomes increasingly urgent with the onset of e- government services in Sri Lanka. The risk of fraud and identity theft increase along with a heightened risk for cyberattacks. The government is in the process of digitising many services and have already digitised some services including online visa forms, electronic customs processes and the acceptance of e-signatures in 2017.

Sri Lanka's e-commerce industry is projected to reach USD 400 million by 2020. As businesses venture on to digital platforms, it is vital for sufficient privacy laws to be in force to secure data as well as to improve business and consumer confidence. Insufficient data protection can create negative market effects by reducing consumer confidence where consumers are unlikely to disclose personal information including financial information. In addition, information and communication technology (ICT) related services including software has become one of the key service sector exports of Sri Lanka. These service exports include automated application testing, infrastructure outsourcing, high end research and development (R&D), enterprise resource planning (ERP), cloud technology and mobile applications. While some of the exports will be subject to compliance with foreign privacy legislation such as the GDPR, national data protection will further reduce the threat of loss of IP.

Additionally, foreign investors will also be concerned about any gaps in data protection laws in the country and a comprehensive yet internationally compatible privacy laws could help attract foreign direct investment (FDI) to the nation.

Although there is legislation around electronic transactions, consumer protection and cybercrime there are no specific laws currently in place for privacy and data protection in Sri Lanka. According to the mapping of data protection and privacy conducted by the UNCTAD in 2019, out of 107 countries mapped 21 percent have no legislation around privacy and data protection of which Sri Lanka falls under. 58 percent have legislation in place while 10 percent of countries mapped have draft legislation.

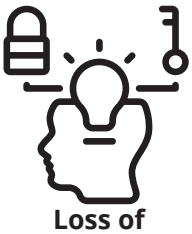
Implications of Insufficient Data Protection and Privacy



Increased Fraud and Identity Theft

Exposure of sensitive and classified information

Influencing National Elections and National Policy



Loss of Intellectual Property

Way Forward

At present, there is no consensus for a single model for data protection laws. However, compatibility is the stated objective of many global and regional data protection initiatives. Sri Lanka's data protection laws need to be drafted with international compatibility in mind to facilitate the smooth cross border transfer of data. For countries without relevant laws in place, the UNCTAD recommends that governments should aim for greater coverage.

Data protection laws need to keep up with new advancements in technologies in order to be effective. Gaps in coverage need to addressed while striking a balance between surveillance and privacy. Moreover, while there are lost business opportunities due to lack of domestic legal protection, overly restrictive protection can act as a barrier to trade. Businesses' compliance burden should be managed with assistance provided for them to overcome any such barriers to adoption. As Sri Lanka embraces new technologies and enters the information society of the 4IR, privacy and data protection are of utmost importance. With the right policies and legislation in place, the economy will be better positioned to reap the benefits offered by the 4IR while mitigating any adverse impacts.

This Policy Insight is based on the comprehensive chapter on "Privacy and Data Protection in the 4IR": State of the Economy 2019 Report' - the flagship publication of the institute of Policy Studies of Sri Lanka (IPS). The complete report can be purchased form the publications section of the IPS.

IPS
100/20, Independence Avenue, Colombo 7,
Sri Lanka
T: +94 11 2143100 / 2665068,
F: +94 11 2665065
www.ips.lk