Contents lists available at JBRI

Journal of Business Research and Insights

journal homepage: https://www.journals.sjp.ac.lk/JBRI

Article

Legal Challenges in Achieving a Business-Oriented Data Protection Ecosystem in Sri Lanka

Abeysekara, T.B.[a*], Dabarera, S.I.[b]

a University of Sri Jayewardenepura

b Attorney-at-Law

To link to this article:https://doi.org/10.31357/jbri.v11i01.8466

ARTICLE INFO

Article History:

Received 14.05.2024
Revised 28.01.2025
Accepted 31.03.2025

Keywords:

Data Protection
Data Protection Ecosystem
Privacy
Common Law
Personal Data Pretection Act No 09 of 2022

ABSTRACT

Data protection refers to the safeguarding and preservation of data from corruption, loss, compromise, or misuse. At the heart of this concept lies the data subject, individuals whose personal information forms the foundation of the data protection framework. In today's rapidly evolving digital landscape, the data ecosystem has expanded significantly, driven by cloud computing, mobile applications, social media, and digital platforms. As a result, consumer and employee data are now collected, analyzed, stored, and shared on an unprecedented scale, increasing the need for robust data protection mechanisms. Simultaneously, tolerance for service interruptions or data breaches has declined sharply.A data protection ecosystem encompasses a comprehensive framework of legal policies, technologies, and best practices that ensure the lawful and secure handling of personal and sensitive data. Despite numerous sector-specific data protection regulations worldwide, many still lack a clear legal definition of 'data'. In Sri Lanka, the urgency for a comprehensive data protection framework has grown alongside increasing digitalization and internet connectivity. Prior to 2022, the country lacked clear legal provisions on data protection. This gap was partially addressed through the enactment of the Personal Data Protection Act No. 09 of 2022. However, the Act has been criticized for ambiguous provisions that may hinder technology-driven entrepreneurship and deter foreign investment.This research explores the legal and practical challenges Sri Lanka faces in establishing an effective data protection ecosystem. It employs doctrinal and comparative methodologies to analyze the Personal Data Protection Act No. 09 of 2022, benchmarked against international standards such as the EU's General Data Protection Regulation (GDPR). Drawing on expert insights and stakeholder feedback, this study offers targeted recommendations to develop a more coherent, business-friendly legal regime. Ultimately, it argues that a transparent, comprehensive, and impartial data protection framework is essential for attracting foreign direct investment in ICT-based industries.

To cite this article: Abeysekara, T.B. and Dabarera,S.I. (2025) Legal challenges in Achieving a Business-Oriented Data Protection Ecosystem in Sri Lanka, Journal of Business Research and Business Research ,11:01, 01-09, DOI: https://doi.org/10.31357/jbri.v11i01.8466

* Corresponding author. Tel: 0718819530; Email: thusitha@sjp.ac.lk
Institution: University of Sri Jayewardenepura

Introduction

This study is significant as it addresses the critical need for a robust and business-friendly data protection legal framework in Sri Lanka, which is essential for safeguarding personal data, fostering digital trust, and attracting foreign direct investments in the rapidly growing ICT sector. The primary objective of this research paper is to examine the legal challenges that Sri Lanka faces in achieving a data protection ecosystem. Data protection is becoming increasingly important in Sri Lanka as the country's digitalization and Internet connectivity accelerate. Internet and social media penetration in Sri Lanka stand at 56.3% and 34.2% respectively and the number of mobile connections is equivalent to 149% of the total population, in the year 2024 (DataReportal.com, 2024). This represents almost 100% growth in the respective sectors compared to where they were a decade ago. With this development, the number of cyber security and privacy incidents in the country has also risen dramatically, from 151 in 2010 to 16,376 in 2020 (Sri Lanka CERT Annual Activity Report, 2020; Kemp, 2020). During the past ten years, the National Center for Cyber Security of Sri Lanka CERT has been constantly publishing red alerts on data movement in cyberspace, indicating various vulnerability issues in search engines, social media platforms, databases (Abeysekara, 2013), virtual private networks, etc (National Center for Cyber Security, 2020). Elimination of the aforesaid problems would not be possible until robust laws on data protection are formulated to keep pace with ICT developments. Data protection is crucial for ICT ventures as it builds trust, ensures compliance with legal standards, and safeguards sensitive information, enabling secure and sustainable business operations.

The enactment of the Electronic Transactions Act No 19 of 2006 (here in after ETA) can be considered as an important milestone in the evolution of the country's ICT legal landscape. ETA was enacted to promote domestic and international e-commerce and e-governance by eliminating legal barriers and establishing legal certainty, through encouraging the use of reliable forms of electronic commerce, and establishing public confidence in the authenticity, integrity, and reliability of data messages, electronic documents, electronic records, and other communications (Sec. 2 of ETA). As a result, both government and private entities including banks, telecommunication service providers, hospitals, educational institutions, and hospitality sector have begun to perform their daily transactions via electronic channels processing vast volumes of sensitive personal data. Even though this transformation has improved the speed and efficiency of services, it has opened doors for personnel data to be misused and misappropriated not only by hackers but also by legitimate users, bringing new challenges for law enforcement authorities.

Moreover, the usage of social media platforms is increasingly growing, resulting in the regular collection and processing of a vast volume of personal data. During the COVID-19 outbreak, people have increasingly become reliant on digital and cloud services such as PickMe and Uber, which resulted in the collection and processing of large volumes of personal information on daily basis (Kerber, 2016). Furthermore, Virtual Private Network ("VPN") has become a remarkably useful tool for online life due to its cost-effectiveness. Ironically, this continued rise in the use of modern technology has opened numerous avenues for third parties to acquire personal data without the owner's consent or knowledge, heightening the vulnerability of such data for misuse, posing threats to individuals' control over their personal data (see the court case-*Durant v Financial Services Authority* [2003] EWCA Civ 1746).

On the other hand, ICT-related services especially data processing services are increasingly becoming one of the key service sector exports of Sri Lanka (Kearney, 2021). According to Kearney, Sri Lanka is emerging as

a favorite location of many global giants for their Information Technology (IT), business process outsourcing (BPO), and other advanced knowledge service centers. Remarkably, Sri Lankan-based firms are providing advanced services including automated application testing, infrastructure outsourcing, enterprise resource planning, and sophisticated accounting services to blue-chip global clients including Google, Microsoft, Lenovo, Nokia, JPMorgan, the London Stock Exchange, Santander Bank, and Emirates (Kearney, 2021). However, potential Sri Lanka has for leveraging from its strategic positioning as well as its relatively high-skilled and low-cost workforce, would not be feasible if the country fails to create a resilient and trusted data protection ecosystem.

Given the foregoing, two legitimate yet conflicting objectives are required to be reconciled when establishing a resilient legal framework for data protection in the face of digitalization in Sri Lanka. On one hand, the protection of personal rights so as to ensure that personal data is handled legitimately and those individuals retain control over their data. On the other hand, facilitating the free flow of personal data to ensure that business entities (digital economy) can process legitimately obtained data without too many obstacles so as to remain competitive in the growing global digital markets (Schwartz, 1994). Accordingly, this paper examines how far the three main divisions of the current Sri Lankan legal system, namely Constitutional Law, Common Law, and statutory law, have succeeded in accomplishing the aforementioned objectives, as well as the inherent flaws therein in developing a resilient data protection ecosystem.

Methodology

This study employs a combination of doctrinal and comparative legal research methodologies. Doctrinal research, or 'library-based research,' is utilized to examine existing legal principles, statutes, case law, and regulations related to data protection in Sri Lanka, with a particular focus on the Personal Data Protection Act No. 09 of 2022. This method enables a detailed analysis of the Act's provisions, their application, and the ambiguities that may pose challenges to business-oriented practices.

A comparative legal research approach is also adopted to evaluate data protection frameworks in other jurisdictions, such as the European Union's General Data Protection Regulation (GDPR) and similar legislation in neighboring countries. This comparison identifies best practices and highlights gaps in Sri Lanka's legal framework, offering insights into potential reforms to establish a business-friendly data protection ecosystem.

Furthermore, a multidisciplinary perspective combining legal, economic, and technological viewpoints ensures a comprehensive understanding of the interplay between data protection laws, business interests, and technological advancements. This integrated approach emphasizes the importance of a holistic and impartial legal regime for attracting foreign direct investments in ICT-driven ventures. The findings aim to offer actionable recommendations for addressing the legal challenges in building a robust data protection ecosystem in Sri Lanka.

Passive Protection for Privacy and Data Protection under Constitutional Law

The Fundamental Rights Chapter of the Constitution of Sri Lanka does not expressly guarantee the right to privacy (Abeysekara & Ranasinghe, 2022; Tznou, 2013). Notwithstanding the unaffirmed status of the right to privacy, it may be, however, inferred as a justifiable limitation on the affirmed constitutional right to access to information enunciated under Article 14 A (1) of the Constitution stipulates that,

"Every citizen shall have the right of access to any information as provided for by law, being information that is required for the exercise or protection of a citizen's right held by:- (a) the State, a Ministry or any Government Department or any statutory body established or created by or under any law; (b) any Ministry of a Minister of the Board of Ministers of a Province or any Department or any statutory body established or created by a statute of a Provincial Council; (c) any local authority; and (d) any other

person, who is in possession of such information relating to any institution referred to in sub-paragraphs (a) (b) or (c) of this paragraph."

Accordingly, privacy is implicitly protected under Article 14A (2) which provide that,

> "No restrictions shall be placed on the right declared and recognized by this Article, other than such restrictions prescribed by law as are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals and of the reputation or the rights of others, privacy, prevention of contempt of court, protection of parliamentary privilege, for preventing the disclosure of information communicated in confidence, or for maintaining the authority and impartiality of the judiciary."

Besides, as argued by Marsoof (2008), the Sri Lankan courts seem to have creatively recognized the right to privacy as a limitation to the freedom of expression guaranteed by Article 14(1) (a) of the Constitution. This is manifested in the verdict of Justice Hector Yapa in *Sinha Rathnathunge v The State* ([2001] 2 SLR 172), in which his Lordship observed that:

> "The press should not seek under the cover of exercising its freedom of speech and expression make unwarranted intrusions into the private domain of individuals and thereby destroy his right to privacy. Public figures are no exception. Even a public figure is entitled to a reasonable measure of privacy."

In view of the above, it may be submitted that recognizing the right to privacy as a justifiable restriction on established constitutional rights such as access to information and freedom of speech, is important from the standpoint of data protection (Susskind, 1987; Waldron, 2012). However, such passive protection cannot be considered as far-reaching enough to protect individuals from contemporary privacy violations and data breaches attributed to modern ICT trends. Moreover, Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), specifically recognize that everyone has the right to be protected from arbitrary and unlawful interference with his or her right to privacy, family, home, correspondence, or reputation. Accordingly, Sri Lanka as a member of the United Nations and a signatory to the ICCPR is bound by the duty to uphold the right to privacy, including the right to privacy of personal information, arising from these two international legal instruments, though so far lagging behind (Sapukotana, 2019). Therefore, as discoursed by scholars, Sri Lanka should preciously consider enshrining the right to privacy and data protection as explicit fundamental rights in the Constitution (Marsoof, 2008).

However, recently introduced Online Safety Act, No 09 of 2024 has taken a step to introduce a possible definition on the concept of 'Privacy' by providing definition and illustrations on the term 'Private Information'. According to the Section 20(2)(a) of this Act, "private information means personal information, including any image, audio or video details, that any person may reasonably expect to remain private, but does not include any information that may be evidence of the commission of any other offence". Under this provision, a person, he or she by themselves, decides what private information is (Illustrations-(a) and (b) of the Section 20 of the Online Safety Act). With compared to the provided interpretations on 'Privacy' by generally all around the world (Warren & Brandeis, 1890), this is a very progressive attempt taken by Online Safety Act. A century ago, Warren and Brandeis argued and suggested the definition of 'Privacy' as 'right to be let alone'. Even at the international level there is no precious definition for the term 'Privacy'. For example, Article 8(1) of the European Convention on Human Rights states that 'Everyone has the right to respect for his private and family life, his home and his correspondence' and Article 12 of the Universal Declaration of Human Rights states that ' Everyone has the right to privacy

and freedom from attacks on their reputation', however, both of them are silent on definition of 'Privacy'. The definition of privacy under Section 20(2)(a) of the Online Safety Act, No. 09 of 2024, lays a strong foundation for recognizing the right to privacy in the Constitution (Article 14 (2)). By focusing on individual autonomy and providing clear illustrations, it introduces a modern and adaptable approach to privacy in the digital age. This progressive definition addresses gaps in international legal frameworks, offering a model for strengthening individual freedoms and aligning Sri Lanka's legal system with global human rights standards.

Post-facto relief to protect privacy and lack of active control over personal data in Common Law

In the Sri Lankan context, the right to privacy and personality, especially for those of a dignitary nature, is protected under Roman-Dutch Law as a 'delict' within the notion of *actio injuriarum* (Marsoof, 2008) and has been developed by case law. In *Nadarajah v Obeysekera* ([1971] 52 NLR 76) the notion of invasion of personal privacy was discussed and the importance of protecting individual's right to privacy and their private space was emphasized. However, due to the various conditions that must be fulfilled for a claim to be successful, this traditional remedy is not widely used (Marsoof, 2008). Moreover, it is restricted to provide relief for invasion of privacy when interference would result in pecuniary damages (Damage on data subject- *Ansari v Google UK Ltd and others* [2022] EWHC 226 Ch; *Lloyd v Google LLC* [2021] UKSC 50).

The collection, processing, and transmission of personal data could involve violation of a person's personality in two ways (Schwartz, 2003). Firstly, a person's privacy could be infringed when true personal information is collected and processed without consent, and secondly, the person's identity could be infringed when false or misleading information is collected and processed (Roos, 2008). Fundamentally, this common-law action tends to provide *post-facto* relief once individual privacy is invaded, which is one aspect of data protection. Yet, it fails to provide individuals an active control over their personal data, allowing them to determine when, how, and to what extent information about them is communicated to others and rights, such as the right to correct incorrect data. Therefore, as discoursed by Justice Saleem Marsoof, it could be confidently submitted that the traditional remedy under *actio injuriarum* is not adequate to deal with the contemporary invasions and affronts against personal information that could take place in the progressively digitizing Sri Lankan society (Marsoof, 2020).

Scattered and Limited Protection of Privacy and Data Protection under Statutory Law

Data protection is a largely unregulated territory in the Sri Lankan legal landscape except for a few provisions in different statutes. In chronological order, reference can be made to the Post Office Ordinance No. 11 of 1908 (as amended) way back in 1908, which could be considered as the first statute to provide positive protection for personal information. Section 75 of the Ordinance imposes punishment for unlawful disclosure of content in a postal article. Almost nine decades later, in 1991, Sri Lanka Telecommunications Act, No. 25 of 1991 ("STA") was enacted which declared an illegal interception of the contents of any telecommunication transmission as an offense punishable by imposing a fine or imprisonment sentence. Section 53 stipulates that " Every person who willfully seeks to intercept and improperly acquaint himself with the contents of any telecommunication transmission not intended for general reception shall be guilty of an offence, and shall be liable on conviction to a fine not exceeding ten thousand rupees or to imprisonment of either description for a term not exceeding six months or to both such fine and such imprisonment.". Even though the STA is the first legislation to recognize interference with electronic data as an offence, regulations on lawful processing of data are hardly found. Another statute relevant in this regard is the Payment Devices Frauds Act No.30 of 2006 which provides an unauthorized disclosure of cardholder information by an employee of an issuer or processor to any third party without the payment device holder's authority as a payment device fraud Sec. 3(1)(d) of Payment Devices Frauds Act).

However, this provision tends to give a third-party greater control over sensitive personal details of a cardholder than the cardholder himself, by acknowledging the payment device holder's consent as a key element in deciding a fraudulent act.

The statute of particular significance for information privacy and protection is the Computer Crime Act No 24 of 2007 ("CCA") enacted in 2007. Even though the Act does not explicitly regulate the processing and movement of personal data, a few provisions protect personal information collected by public and private entities that offer platforms for customers to communicate through computer systems (Abeysekara, 2015). These protections include *inter alia* recognizing unauthorized access to a computer (Sec. 3 of CCA), illegal interception of data (Sec. 8 of CCA), and unauthorized disclosure of information (Sec. 10 of CCA) as offences punishable by penal sanctions and compensation to the victim (Sec. 14 of CCA). When examining these provisions, it is evident that even though, CCA endeavors to safeguard against unlawful invasion of personal data in electronic systems, as argued by Marsoof, such protection is insufficient to deal with impediments to free movement on the Internet and invasion of territorial privacy resulting from the use of applications like cookies, web bugs and spam (Marsoof, 2007). This view would appear to be the account favoured by Ariyaratna (2019) and Abeysekara (2015) who argues that even though the CCA aims to safeguard privacy and personal data in the electronic environment, the basic security provided by the Act is insufficient to resolve the overall privacy and data protection concerns in online transactions.

Notably, the Right to Information Act No. 12 of 2016 was enacted in 2016 in order to enforce the fundamental right to access to information enunciated under Article 14A (1) of the Constitution of Sri Lanka. Under Section 5(1)(a) of the Right to Information Act, the request for access to a citizen's personal information may be denied if such request has no connection to a public activity or which would cause unwarranted invasion of the individual's privacy unless the larger public interest (for practical example- *Hájovský v. Slovakia* [2021] ECHR 591) justifies the disclosure or the person concerned consents to such disclosure [The case mainly concerns an alleged breach of the applicant's right to private life under Article 8 of the Convention by the publication of, *inter alia*, photographs of him, and the ensuing domestic court decisions dismissing his related claims]. This section tends to offer individuals a certain degree of control over their personal information. Hence, it could be considered a somewhat positive step towards the protection of personal information, in the absence of specific legislation to enshrine data protection in Sri Lanka.

In the light of the above, before the Personal Data Protection Act No 09 of 2022 came into force, it could be submitted that data protection was largely unregulated in Sri Lanka except for a few legal provisions in different statutes that provide limited protection against illegal invasion of personal information, unlawful access to computers, and illegal interception of contents of telecommunication transmission. However, when their legal effects are collectively considered, those statutory provisions neither provide a definition for the term 'data' nor specific provisions for the regulation of the collection, storage, processing, and transmission of personal data.

Grey areas in the Personal Data Protection Act No 09 of 2022

The long-standing vacuum in law for data protection was attempted to be addressed when the Data Protection Drafting Committee appointed by the Ministry of Digital Infrastructure and Information Technology (here in after MDIIT) released a draft Personal Data Protection Bill (here in after PDPB) on September 24, 2019. However, the PDPB had been criticized for having ambiguous provisions that are deterrents to Foreign Direct Investments (here in after FDI) in technology-driven ventures. Sections 26(2), provisions of Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of the Personal Data Protection Act, for examples, empower the Minister to issue processing regulations from time to time in

consultation with the Data Protection Authority (here in after DPA). This could allow the Minister to change different processing grounds frequently, resulting in legal uncertainty that could stymie FDIs. Another provision that raises concern is the requirement for the controllers to conduct Data Protection Impact Assessments (here in after DPIAs) when the processing is likely to result in a high risk to the rights of the data subjects under any written law (Sec. 12(1)(c), 20(5)(d) and generally Sec. 24 of Personal Data Protection Act, No 9 of 2022). DPIAs should be conducted if the processing is for profiling, large-scale processing of special categories of personal data, monitoring of public space or telecom networks, or any other activity that may be prescribed as processing. This requirement is particularly broad because the possible risks to data subjects *under any written law* are hard to foresee, requiring a controller to perform DPIAs in numerous situations at a high cost and extended time. Besides, the DPIA must be furnished to the DPA, which has the power to halt the processing activity if it deems such processing to be 'high risk' after mandatory consultation. Instead of strengthening the accountability-based approach, this could transform DPIAs into a preventative management tool, slowing the delivery of innovative services. These procedural red tapes could hinder FDIs.

Furthermore, the Personal Data Protection Act tends to place the same degree of obligations on processors as it does on controllers. The processors must adhere to the processing requirements specified in four of the five Schedules in the Act. For processors who do not comply with those conditions, a maximum fine of ten million Sri Lankan rupees may be imposed (Sec. 38(1) of Personal Data Protection Act, No 9 of 2022). This onerous regulatory control over processors exceeds international norms and may deter investment in the data processing and outsourcing industries in the country. Another area that claims an amendment is the composition of the DPA. The Minister may designate any statutory body or other government institution constituted under any written law. Moreover, the Cabinet of Ministers has the authority to issue directions to the DPA on how to discharge its functions. This expansive authority firmly indicates that the Government would have considerable control over the DPA, which could undermine its legitimacy as an independent body. This is in contrast to the international standards which mandate an independent supervisory body. Monitoring by an independent regulatory body is essential to ensure that a fair and effective data protection mechanism is enforced in the country to attract FDIs.

Despite the above backlashes, the Personal Data Protection Act, No 9 of 2022 tends to prescribe measures to protect the personal data held by banks, telecommunication service providers, hospitals, and other entities that collect and process personal data. Nonetheless, the Legislature's effort should be applauded, and this should be used as a steppingstone towards improved legislation that complies with the European order's such as General Data Protection Regulation (GDPR) and related court cases adequacy standards for smooth cross-border data flows (Koops, 2014; Wachter & Mittelstadt, 2019).

Conclusion

The current state of privacy and data protection laws in Sri Lanka reveals significant gaps and challenges, as discussed in this article. It is evident that the country lacks adequate constitutional protection for privacy and substantive legislation to regulate data protection, relying instead on limited provisions such as the common law notion of *actio injuriarum* and fragmented statutory measures. While Sri Lanka has introduced modern ICT laws like the Electronic Transactions Act and the Computer Crime Act, these advancements have not been matched by efforts to establish a comprehensive data protection regime. Consequently, Sri Lankan citizens face considerable risks of their personal data being misused by third parties without consent or knowledge, undermining trust and security in the digital landscape.

The lack of strong data protection laws also limits Sri Lanka's ability to maximize the potential of its existing ICT framework. Although the country became the first South Asian nation to ratify the Budapest Convention in 2015, it has not fulfilled its obligations to implement

data protection legislation that meets international adequacy standards. This failure restricts the seamless flow of trans-border data and creates barriers to international commerce. Such inadequacies undermine investor confidence in the country's ICT sector, posing challenges to cross-border data exchange and hampering economic growth.

In conclusion, the article highlights the urgent need for Sri Lanka to adopt and implement a holistic data protection regime that aligns with globally recognized standards. Such reforms are essential to build trust among individuals and investors, foster a secure digital environment, and establish a resilient data protection ecosystem that supports sustainable ICT development and international collaboration. Addressing these gaps will enable Sri Lanka to fully capitalize on the opportunities presented by its digital transformation while safeguarding the rights and privacy of its citizens.

References

Abeysekara, T.B., (2013). *A Proposal for the Protection of Digital Databases in Sri Lanka* (PhD Thesis-University of Exeter UK).

Abeysekara, T.B., (2015). Computer Crimes; Endless Race of Road Runners, *Judicial Service Association Law Journal*, 3, 127.

Abeysekara, T.B., Ranasinghe, A.E., (2022). Holistic Approach in Introducing Proper Legal Framework to Regulate Data Protection and Privacy in Sri Lanka, *Vidyodaya Journal of Management*, 8(1), 170.

Ansari v Google UK Ltd and others [2022] EWHC 226 (Ch).

Ariyaratna, B.A.R.R., (2019). Are Consumers Safe Online? A Critical Analysis of Sri Lankan Legal Regime on Online Consumer Protection', X, *The Junior Bar Law Journal* <https://www.juniorbarbasl.lk/volumex.html >accessed 06 March 2024.

Computer Crime Act, No. 24 of 2007.

Constitution of the Democratic Socialist Republic of Sri Lanka-1978.

DataReportal web <https://datareportal.com/ > accessed 14 May 2024.

Durant v Financial Services Authority [2003] EWCA Civ 1746.

Electronic Transactions Act, No. 19 of 2006.

European Convention on Human Rights (ECHR; formally the Convention for the Protection of Human Rights and Fundamental Freedoms) – 1953.

Fernando, J., and Alexander Seger, (2016). 'Budapest Cyber Crime Convention and its Impact on the Sri Lankan ICT Legal Regime', *The Bar Association Law Journal*, XXII, 277.

Hájovský v. Slovakia [2021] ECHR 591.

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

Kearney, 'Competitive Benchmarking: Sri Lanka Knowledge Services' (*www.es.kearney.com*) <https://www.es.kearney.com/web/global-business-policy-council/article/?/a/competitive-benchmarking-sri-lanka-knowledge-services> accessed 06 March 2023.

Kemp, S., 'Digital 2020: Sri Lanka' (*www.datareportal.com*, 18 February 2020)<https://datareportal.com/reports/digital-2020-sri-lanka> accessed 29 December 2024.

Kennedy, G., Doyle, S., & Lui, B., (2009). Data protection in the Asia-Pacific region, *Computer Law & Security Review*, 25(1), 59-68.

Kerber, W., (2016). Digital markets, data, and privacy: competition law, consumer law and data protection. *Journal of Intellectual Property Law & Practice*, 11(11), 856-866.

Kira, B., Sinha, V., & Srinivasan, S. (2021). Regulating digital ecosystems: bridging the gap between competition policy and data protection. *Industrial and Corporate Change*, 30(5), 1337-1360.

Koops, B. J., (2014). The trouble with European data protection law, *International data privacy law*, 4(4), 250-261.

Lloyd v Google LLC [2021] UKSC 50.

Marsoof, A., (2007). 'Privacy Related Computer Crimes: A Critical Review of the Computer Crimes Act of Sri Lanka' *Sri Lanka Law College Law Review* 5.

Marsoof, A., (2008). 'The Right to Privacy in the Information Era: A South Asian Perspective', *Script-ed* 5(3), 553, 559.

Marsoof, S., 'E-Commerce & E-Governance – Some Pertinent Issues' <https://www.academia.edu/12868743/E-Commerce_and_E-Governance_-

_Some_Pertinent_Issues> accessed 22 May 2024.

Nadarajah v Obeysekera [1971] 52 NLR 76.

National Center for Cyber Security – Sri Lanka CERT, 'Alerts' (*www.cert.gov.lk*, 08 December 2020)<https://www.cert.gov.lk/alerts.php> accessed 29 December 2024.

Online Safety Act, No. 9 of 2024.

Payment Devices Frauds Act, No.30 of 2006.

Personal Data Protection Bill - L.D.O. 19/2019.

Post Office Ordinance, No. 11 of 1908 (as amended).

Right to Information Act, No. 12 of 2016.

Roos, A., (2008). 'Personal Data Protection in New Zealand: Lessons for South Africa?', *PER / PELJ* 11(4), 62 <https://www.researchgate.net/publication/318210782_Personal_Data_Protection_in_New_Zealand_Lessons_for_South_Africa/link/595d1610aca27230850cfad1/download> accessed 26 December 2024.

Sapukotana, U., 'Protecting eHealth Information Privacy: Towards a Legal Framework for Sri Lanka' (PhD thesis, General Sir John Kotelawala Defence University 2019) 148.

Schwartz, P. M., (2003). Property, privacy, and personal data. *Harvard. Law Review*, 117, 2056.

Schwartz, P. M., (1994). European data protection law and restrictions on international data flows, *Iowa Law Review*, 80, 471.

Sinha Rathnathunge v The State [2001] 2 SLR 172.

Sri Lanka Computer Emergency and Readiness Team, 'Sri Lanka CERT Annual Activity Report 2020' (*www.cert.gov.lk*) <https://cert.gov.lk/documents/Sri_Lanka_CERT_Annual_Activity_Report_2020.pdf > accessed 14 November 2024.

Sri Lanka Telecommunications Act, No. 25 of 1991.

Susskind, R., (1987). Expert Systems in Law and the Data Protection Adviser *Oxford Journal of Legal Studies*, 7(1), 145–151.

Tzanou, M. (2013). Data protection as a fundamental right next to privacy? 'Reconstructing'a not so new right. *International Data Privacy Law*, 3(2), 88-99.

Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR).

Wachter, S., & Mittelstadt, B., (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI *Columbia Business Law Review*, 494.

Waldron, J., (2012). How Law Protects Dignity The Cambridge Law Journal, 71 (1), 200-222.

Warren, S., Brandeis, L., (1890). The Right to Privacy *Harward Law Review*, 4, 193.