KDU Law Journal
General Sir John Kotelawala Defence University, Sri Lanka

Volume 02, Issue II
September, 2022
ISSN 2783-8870

A Critical Analysis on the Adequacy of the Existing Legal Framework for Safeguarding E-Consumer Rights in Sri Lanka

Shaveen Sachintha[1]

Abstract

With the rapid growth of e-commerce, people tend to engage with e-transactions more. As a result of the complex nature of online transactions, consumers are facing severe challenges, and their privacy and data protection rights are being violated continuously. Therefore, sufficient measures must be taken to safeguard the rights of e-consumers. In this paper, the Author analyzes the legal instruments of Sri Lanka which can be utilized to protect the rights of e-consumers. However, when considering the existing legal framework of Sri Lanka related to the protection of e-consumer rights, it is evident that Sri Lanka has not facilitated sufficient protection for the customers on an e-platform. It can be understood by the fact that no legal instrument accords express protection for online consumers. Therefore, the Author discusses challenges that e-consumers are facing in e-transactions and certain instances where consumer rights become problematic. Moreover, the author compares and contrasts the existing legal framework in Sri Lanka with legal frameworks of developed and developing jurisdictions to suggest appropriate recommendations to Sri Lankan law. Finally, the author discusses the initiatives taken by Sri Lanka in order to safeguard the interests of e-consumers. The author uses the qualitative approach and mainly relies upon secondary data.

Keywords: *E-Consumer, Consumer Rights, Consumer Protection, E-Contract, Data Protection, Electronic Transactions, Online Privacy.*

[1] LL.B (Hons) (Jaffna), Assistant Lecturer, Department of Law, University of Jaffna

Introduction

When analyzing the existing legal framework of Sri Lanka, there is no any express legal basis regarding online consumer protection. Information technology and consumer law related legal frameworks provide implied legal protection for e-consumer rights. Importantly, the Electronic Transaction Act[2] (ETA) and the Computer Crime Act[3] (CCA) were enacted to strengthen the legal certainty of the e-commerce sector and penalize the violations in cyberspace. Consumer Affair Authority Act[4] (CAAA) was enacted to address the issues in commercial trade and to protect consumer rights, though there is no any specific indication about online consumers. However, it is questionable whether these existing laws adequately address the protection of e-consumers.

In 2019, the Data Protection Bill was presented to overcome the challenges in personal data and privacy protection. The Bill seeks to establish a "Data Protection Authority" and encourage online consumers to engage with e-commerce. Moreover, in 2019, the Cyber Security Bill was presented and it is concerned with the strengthening of the payment security on e-platforms. Further, it establishes a "Cyber Security Agency" to protect essential services from cyber-attacks. Importantly, the Sri Lankan parliament enacted the Data Protection Act aiming to promote a digital economy while preserving the privacy of individuals in 2022. However, the Cyber Security Bill is not incorporated to Sri Lankan legal framework yet.

- Protection of e-consumer rights under the existing legal framework of Sri Lanka

According to Section 3 of ETA, the validity and enforceability of electronic records were legally recognized, and records cannot be ignored just because it is in e-form. Moreover, admitting the legal recognition of e-signature under Section 7 enhances the public confidence in e-commerce[5]. Importantly Section 11 certifies the legal validity and enforceability of e-contracts and paper-based contracts.

[2] The Electronic Transactions Act No. 19 of 2006
[3] The Computer Crime Act, No.24 of 2007
[4] The Consumer Affairs Authority Act No.09 of 2003
[5] Kariyawasam K, "The Growth and Development of e-Commerce: An Analysis of the Electronic Signature Law of Sri Lanka" Information & Communications Technology Law Journal, (2008).

ISSN 2783-8870

Although the ETA affirms online transactions are recognizable and accepted, it fails to provide any specific legal basis for the protection of e-consumer rights. The ETA is silent regarding personal data and privacy protection in e-transactions[6]. Furthermore, it failed to provide any regulatory mechanism to protect online consumers when they enter into e-contracts.

The preamble to the CCA sets out the objectives of the Act as identification of computer crimes, providing procedures for crime investigation and prevention of such crimes. Therefore, penalization of violations in cyberspace gives some protection to online consumers. Sections 8 and 10 provide basic safeguards for personal data and privacy protection by recognizing the illegal interception of data and unauthorized disclosure of information as computer crimes.

Although there is apparent protection, these provisions are not adequate to address data and privacy protection issues in e-transactions. Importantly, when the consumer deals with technological applications like cookies, spam, web bugs etc. this protection is obviously insufficient[7].

As the major consumer protection legal framework of Sri Lanka, the CAAA established the Consumer Affairs Authority to safeguard the general protection of consumers and traders. According to Section 75, the interpretation to the word 'Consumer' does not make any special reference to consumers of online trading. But the interpretation of the term 'Service' includes field of Information Technology and Communication. Although it can be argued that the interpretation implies 'online consumers', the law needs more clarification regarding this definition.

The CAAA does not impose any obligation upon sellers to disclose relevant information such as the identity of the seller, geographical address, arrangement of payment, delivery performance etc. Moreover, the law does not address the withdrawal rights of the online consumers called as 'Cooling Off Period'[8]. Although Part II of the CAAA broadly address the regulation of

[6] Madugalla KK, "Right to Privacy in Cyberspace: Comparative Perspectives from Sri Lanka and Other Jurisdictions," Kelaniya International Conference on Information and Technology (University of Kelaniya 2016).

[7] Marsoof A, "Privacy Related Computer Crimes; A Critical Review of the Computer Crimes Act of Sri Lanka" (2007) 5 Law College Law Review 1

[8] Cooling off period means the consumer will be given withdrawal rights to leave the contract without paying any compensation within a certain time period.

trade, it failed to confer any authoritative power specifically on Consumer Affairs Authority to regulate online trade. Further the Act does not address new concepts like contracts relating to digital contents[9] and the Consumer Affairs Authority and Consumer Affairs Council are not adequate to resolve disputes in online trading platforms.

In 2020, the Consumer Affairs Authority raided '*Kapruka*', an online retail store upon consumers' complaints regarding violations of maximum retail prices by utilizing the given powers under the CAAA[10].

Moreover, the Unfair Contract Terms Act[11] can be applied to mitigate the arbitrariness of sellers imposing terms on e-contracts as they wish. Part VI of the Telecommunication Act[12] also provides some implied protection to the online privacy of e-consumers.

According to the Data Protection Act of Sri Lanka, the Ministry of Digital Infrastructure and Information Technology is required to establish a Data Protection Authority to deal with privacy protection in online or offline media. Moreover, the Authority's power and functions are expressly listed in the Act. Importantly, the Authority is empowered to receive complaints regarding unauthorized or harmful personal data processing. Even without receiving a complaint, if the authority anticipates that there may be a violation of personal privacy, the Authority is able to commence an investigation under the legal framework of the Act.

The requirements and procedure of the investigation process and powers of the chairman and members of the authority during the investigation process were expressly stated in the Act. After the investigation process, the authority shall produce directives to both parties and, by considering the nature and gravity of the violation, the Authority shall file a case before a Court of Law. When the Authority issues directives with regard to any complaint, all the parties relating to complaint are bound by such directives. If any person fails to adhere to the directives of Authority without any legitimate excuse, such

[9] Perera WC, "Beware If You Are a 'Digital Consumer'- Intangible Digital Goods and Consumer Protection in Sri Lanka," (General Sir John Kothalawala Defence University 2018).
[10] Consumer Affairs Authority Raids Kapruka Office for Violating Regulations and Unethical Business Practices <https://www.asianmirror.lk/news/item/31064-update-consumer-affairs-authority-raids-kapruka-office-for-violating-regulations-and-unethical-business-practices> accessed 25 April 2022
[11] The Unfair Contract Terms Act 26 of 1997
[12] The Sri Lanka Telecommunications Act,No. 25 of 1991

ISSN 2783-8870

person shall be guilty of an offence.However, it is clear that the existing legal frame work of Sri Lanka does not adequately address the issues of online consumers. Importantly, Section 3 of the Civil Law Ordinance[13] permits the adoption of English common law, rules of equity and certain statutes in the absence of Sri Lankan legislation. Therefore, the protection of e-consumer rights under English Law can be concerned for safeguarding the e-consumer rights in Sri Lanka to some extent.

Due to the major drawbacks in the legal system and the complex nature of online trading, consumers' rights are severely violated. Therefore, it is important to discuss some stages where the consumer rights have become problematic in the online medium.

- The instances where e-consumer rights become problematic

Basically, we can identify three stages where consumer protection issues arise and consumer rights would be affected in an e-platform.

- Pre-purchasing Stage - Information Asymmetry
- Purchasing Stage - Online Privacy / Payment Security
- Post Purchasing Stage - Cross-Border Consumer Complaints / Redress Mechanism

Information Asymmetry means one party to the contract possesses greater material knowledge than the other party in an economic transaction. In online trading, consumers deal with unknown sellers and vendors. Consumers know only the information which are disclosed by sellers. Asymmetric information may lead to fraudulent consequences and the consumer may be misled because of the insufficiency of information[14].

Online Privacy is one of the major areas where consumer rights would be violated. During the registration and ordering process in online trading, consumers are required to provide personal information such as name, email address and credit card number and so on. Importantly, when consumers engage in online transactions, their IP Addresses[15] can be captured and this can be used to gather

[13] The Civil Law Ordinance No.5 of 1852
[14] Asymmetric Information by ANDREW BLOOMENTHAL (para.7)
[15] An IP address is an address assigned to a computer that is connected to the Internet. Using an IP address, one computer can request or send information to the other.

the information regarding online activities of consumers[16].

E-consumers make their payments electronically in internet-based shopping and banking. Therefore, several issues have arisen regarding Payment Security in online platforms[17]. In cyberspace there are thousands of viruses and malicious software used to attack online payment systems by capturing banking passwords. As an example, the *Zeus Trojan*[18] was used to attack mobile banking payment systems.

In online shopping, consumers cannot physically inspect the goods and they have to pay before receiving the order. That is why a Redress Mechanism should be established to safeguard consumer rights. The redress mechanism deals with consumers' right to express dissatisfaction, the right to make complaints and receive feedback and compensation[19]. The absence of a proper redress mechanism would undermine the consumer rights and trustworthiness of e-commerce.

Cross-Border Consumer Complaints arise when the consumer makes a complaint against the e-seller who is overseas. When the seller does not provide relevant information like the identity of the seller, geographical address, delivery performance etc., it would be a challenge to the consumer to make a complaint. Usually, a contract will be governed by the country's law where the goods are supplied. It will be more problematic to the consumer if legal action has to be taken in the Courts of the seller's country.

- Comparison with other jurisdictions

Different countries have taken various steps to overcome the above issues and safeguard e-consumers rights on e-platforms. I will analyze how the legal frameworks of the United Kingdom and South Africa deal with e-consumer rights protection.

The United Kingdom as a developed country has taken major steps to safeguard

[16] Internet Privacy in E-Commerce: Framework, Review, and Opportunities for Future Research-Conference: Hawaii International Conference on System Sciences, Proceedings of the 41st Annual

[17] Bogdan-Alexandru Urs, 2015. "Security Issues and Solutions In E-Payment Systems," FIAT IUSTITIA, Dimitrie Cantemir Faculty of Law Cluj Napoca, Romania, vol. 9(1), pages 172-179

[18] V. Goyal, Dr.U.S.Pandey, S. Batra,"*Mobile Banking in India: Practices, Challenges and Security Issues" International Journal of Advanced Trends in Computer Science and Engineering,* pp. 56-65.

[19] Edwards, L., and Wilson, C. 2007. *"Redress and Alternative Dispute Resolution in = EUCross-Border E-business Transactions," International Review of Law, Computers & Technology''*, pp. 315-33.

ISSN 2783-8870

the e-consumer rights. They were bound to follow the Consumer Rights Directive [20] of the European Union. Therefore, the United Kingdom introduced Consumer Contract Regulations[21] (CCR) and Consumer Rights Act[22] (CRA) by adhering to the directive.

The CRA provides a very broad interpretation to the word 'consumer' where both offline and online consumers rights are subjected to protection. Importantly, suppliers are strictly required to disclose the relevant information to consumers under Sections 10 and 11 of the CRA. Moreover, Schedules 1 and 2 of CCR also provide that traders must disclose the information to the consumer, especially the identity of the trader and his geographical address. In Sri Lanka, there are no such requirements and Section 26 of CAAA merely states that traders should display the price list.

In order to secure the personal data of consumers, the United Kingdom introduced separate legislation called Data Protection Act[23]. It requires the data controllers to use such sensitive data lawfully and fairly. Moreover, Section 27(4) of the Act for prohibited retaining such data more than necessary. Section 20 of the CRA ensured the consumers' right to reject the goods by granting cooling-off period.

Moreover, the United Kingdom introduced an Alternative Dispute Settlement Mechanism for online consumers under Regulation 2015[24]. Section 19A of Regulation 2015 required the online traders to use the alternative dispute settlement procedure. In Sri Lanka, there is no such dispute settlement mechanism and e-consumers have to complain to Consumer Affairs Authority which has not been conferred with any specific authority to deal with e-transactions.

South Africa as a developing country has taken some salutary steps to overcome the issues relating to consumer rights and safeguard those rights. In South Africa, the Electronic Communication and Transaction Act (ECTA) [25] and the Consumer Protection Act[26] (CPA) are prominently dealing with the rights of online consumers.

[20] Directive 2011/83/EU on Consumer Rights.
[21] the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013
[22] The Consumer Rights Act 2015 became law on 1 October 2015.
[23] Data Protection Act 1998
[24] The Alternative Dispute Resolution for Consumer Disputes (Amendment) Regulations 2015
[25] Electronic Communications and Transactions Act, 2002. No. 25 of 2002.
[26] Consumer Protection Act No. 68 of 2008

The ECTA contains a separate chapter that is completely associated with consumer protection in e-platform. Section 42(1) affirms that the Chapter VII of the Act specifically applicable to online transactions. Importantly, Section 43 required the suppliers to provide all relevant information to consumers, and the consumer was granted the right to review the entire transaction and withdraw from the transaction. Moreover, under Section 43(5), the supplier is required to utilize a sufficiently secure payment system, otherwise he will be liable for damages under Section 43(6). Section 44 of the Act certified consumers' withdrawal rights by providing a cooling-off period. In the ETA of Sri Lanka, even though there are some implied provisions regarding consumer rights protection, it does not specifically cover the broader area of e-consumer rights like the ECTA of South Africa.

In order to safeguard the data and privacy of online consumers, the Protection of Personal Information Act[27] was enacted. It provides certain procedures to protect the privacy and data of e-consumers. Moreover, Chapter VIII of ECTA and Sections 11 and 12 of CPA impose certain regulations to protect e-consumer privacy in e-platform.

The CPA of South Africa further ensured the fundamental rights of online consumers. It recognized different kind kinds of consumer rights such as the right to disclosure and information, rights to fair and responsible marketing, the right to demand quality goods and quality service and so on. Under Section 41, sellers are prohibited from providing misleading/ fraudulent representations as to goods. Section 48 prohibited the seller to incorporate unreasonable terms into the contract. If there is any violation of rights, consumers can refer the dispute to the National Consumer Tribunal[28], Provincial Consumer Court[29] or to National Consumer Commission[30].

As a country, Sri Lanka does not have an effective National Privacy Policy to safeguard the privacy of people either online or offline. When we consider countries like Australia, Canada, United Kingdom, it is clear that they have expressly recognized National Privacy Policy either by statutory law or by regulations of relevant authorities. Moreover, India as a developing country,

[27] Protection of Personal Information Act 4 of 2013
[28] Section 69(a) of the Consumer Protection Act -2008
[29] Section 69(c)(i) - (iii) of the Consumer Protection Act -2008
[30] section 69(d) of the Consumer Protection Act -2008

ISSN 2783-8870

in 2011 published by a Gazette "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules" which recognized the five major national privacy policies in India[31].

According to IAPP[32], National Privacy Policy is an internal document of the country which regulate and lay down basic principles of how a 'Data Fiduciary' process, use and disclose data of 'Data Principle 'obtained by way of website or application. Although Sri Lanka has few implied statutory provisions, there is no any express legal frame work or National Privacy Policy. Therefore, I hereby recommend that the Sri Lankan Government and proposed 'Data Protection Authority' should take necessary steps to formulate the National Privacy Policy of Sri Lanka.

When the government formulates the National Privacy Policy of Sri Lanka, the following key principles should be taken into consideration.

- Collection - The National Policy must address how the personal data should be collected through online or physically for legitimate and fair purposes within the territory of Sri Lanka.
- Use and Disclosure - The National Policy must address how the duly collected data is utilized, processed or disclosed within the territory of Sri Lanka or outside. It is important to regulate that data can only be used for any legitimate purposes for which such data is collected.
- Data Security - The National Policy must enumerate the basic steps and means that should be taken to protect data from misuse and unauthorized access or disclosure.
- Accountability - The National Policy must address the responsibilities of relevant authorities regarding protection and promotion of security of personal data.

In the Sri Lankan legal framework, it is clear that we cannot find broader legal protection for e-consumer rights like in the UK and South Africa. However, some initiatives are taken by Sri Lanka to safeguard the interests of local e-consumers.

In 2018, Sri Lanka attempted to update e-commerce consumer protection laws

[31] G.S.R. 313(E) dated 11 April 201
[32] International Association of Privacy Professionals

covering the pre-purchase stage, purchase and post-purchase [33]. Although, the government agreed to update the law on e-commerce according to ITC, it was not implemented.

When comparing the Data Protection Law of Sri Lanka with Singapore, they established a Personal Data Protection Commission to deal with the protection of individual privacy. It also possesses identical powers and functions as Sri Lankan Authority. But unlike in Sri Lanka, Singapore established a separate body called "Data Protection Appeal Committee". Where any individual is dissatisfied with the decision of the Commission, he/she can appeal to Appeal Committee before going to court. In the United Kingdom "The Information Commissioner" was established under Data Protection Act, 2018. This statutory body also functions similarly to, and possesses identical powers to the Sri Lankan Authority. Moreover, the Data Protection Act of the United Kingdom describes the international role of the Information Committee to provide proper safeguards to the privacy of individuals which should be included in the Sri Lankan Act. However, the adoption of the Data Protection Act into Sri Lankan legal framework can be considered as a major step of safeguarding personal information of e-consumers.

Recommendations and Conclusion

This paper thoroughly discusses the inadequacy of the Sri Lankan legal framework to safeguard the e-consumer rights and the instances where consumer rights would be problematic on e-platforms. Moreover, it was analyzed how the existing law should be updated and amended by referring to the United Kingdom, South Africa and well-updated legal frameworks of other jurisdictions. Therefore, the Sri Lankan government should take immediate steps to ensure the e-consumer rights by strengthening the legal framework and the right to the protection of personal information should be guaranteed as a constitutional right of Sri Lanka.

E-consumers also should take some precautions when they deal with e-platforms. The Government should conduct awareness programs and e-consumers should be given instructions as to how their rights can be violated on e-platforms and how they can be protected from those violations. Then

[33] Sri Lanka updating e-commerce consumer protection laws < https://economynext.com/sri-lanka-updating-e-commerce-consumer-protection-laws-11436/ > accessed 25 April 2022

ISSN 2783-8870

e-consumers also will have some responsibility not to engage with 'Risky Online Activities'.

Information Technology and Consumer related laws of Sri Lanka only provide implied protection for e-consumer rights. However, when we compare the Sri Lankan legal framework with the legal frameworks of the United Kingdom and South Africa, it is obvious that mere implied protection will not be adequate to safeguard consumer rights on e-platforms. As a result of this inadequate legal protection, e-consumers are facing severe challenges and their rights are being violated continuously. Although the Sri Lankan government has taken some initiatives to strengthen the legal framework on e-consumer protection like enacting a legislation on privacy protection, they are yet to be implemented. Therefore, Sri Lanka has a major task to strengthen the legal framework on e-commerce and enhance consumers' protection and confidence on e-transactions.