Banning Social Media for the Purpose of National Security; A Cry out for a Regulated Legal Mechanism to Monitor Social Media Platforms.

MASSS Gunasekara[1]

[1]*Undergraduate of General Sir John Kotelawala Defence University*
[#] Corresponding author; <masssgunasekara@gmail.com>

Abstract *- Technological advancements have paved the way to strengthen the rights of the public. Equally these rights are abused when they are transmitted to the virtual medium. The rights guaranteed by International Convention on Civil and Political Rights (ICCPR) now extend even to the cyber space. Due to new forms of communication modes like social media, boundaries of freedom of expression are unleashed. However, the same rights are frustrated due to unregulated filtering, blocking, banning and even by denying access to information via social media by governments for the purpose of national security. Recently, Sri Lanka experienced threats to national security due to unregulated use of social media which resulted in barricading the access. Therefore, the main objective of this paper is to address the need for a separate legal mechanism to regulate and monitor information shared via social media platforms active in Sri Lanka, in order to prevent abrupt blocking which will in turn lead to banning. Further, this study highlights the importance of striking a balance between freedom of expression via social media and national security. To that end it suggests an approach which extends beyond existing legislations, connecting the government, social media platforms and citizens. The paper will follow black letter approach and the recommendations to the regulatory mechanism will be provided with special reference to India and United Kingdom (UK).*

Keywords— **social media, national security, freedom of speech**

I. RESEARCH PROBLEM

The problem addressed by this paper is the need for a separate legal mechanism to regulate social media platforms. In addressing the above-mentioned issue, this research intends to;

- Analyse whether existing legislations suffice for the regulation of social media and the authority of the government to block/ban social media for national security in Sri Lanka.
- Discuss how India and UK regulate social media to ensure national security.
- Provide recommendations for a separate legal mechanism to regulate and monitor social media to strike a balance between freedom of expression via social media and national security.

I. INTRODUCTION.

In the year 2019, immediately after the Easter Sunday Attack social media platforms were blocked three times continuously within one month. Regardless of the block misuse of social media continued. Unknowingly it only led for a violation of freedom of expression due to unregulated use of social media.

Social media is another media outlet, which needs to be regulated by law. Totally banning or blocking this avenue is clearly an arbitrary use of power resulting from the lack of sufficient mechanism to regulate it. Therefore, the paper intends to focus on the importance of striking a balance between freedom of speech while assuring national security.

II. METHODOLOGY

This study is conducted in form of a library research based on both primary and secondary data. It draws from both Sri Lankan legislations (Constitution, Computer Crimes Act No. 24 of 2007, Public Security Ordinance No. 25 of 1947, Telecommunication Act No. 27 of 1996 and Intellectual Property Act No. 36 of 2003) and foreign legislations (Indian Information Technology Act No. 21 of 2001 and Computer Misuse Act No. of 1990). Further, case laws and *opinio jurist* will be used to support the arguments.

Moreover, this research is guided by studies which have already conducted in the fields of social media, freedom of expression and national security. Journal articles, conference papers and web resources will supplement the discussion.

The research question is addressed by comparing Sri Lanka with other jurisdictions specifically India and United Kingdom (UK). How countries like India address situations in relation to social media and national security how Information Technology Act of 2000 tackle the situations will be analysed. Recommendations to a new legal

framework is discussed by referring to the new UK proposal (Online White Harm Paper).

Mainly the research is centred in addressing question, 'is banning/blocking of social media the only remedy available to regulate social media at a time of emergency?' or 'is it mere a slippery slope due to the lack of sufficient mechanism to regulate social media in Sri Lanka?'.

III. LITERATURE REVIEW

There has been an escalating level of research conducted on the fields of Social Media, Freedom of Expression and National Security.

Jaccopo Coccali, The Challenges on New Technologies in the Implementations of Human Rights: An analysis of some critical issues in the implementation (2017) states that same rights which people have offline must also be protected online. The writer recognises the expansion of rights of people (ex: freedom of expression) with the development of new technologies. It shows the gap existing between technical progress and development of legal implications. He provides that unregulated technical expansion will have adverse consequences on human rights. In re-interpreting freedom of expression in light of digital innovations, he quotes Balkin and states freedom of expression is aimed at establishing democracy. Further, he accepts the vulnerability of human rights to be exposed to unpredicted threats due to unregulated use of technologies. Coccali has centered his study on addressing whether today's regulatory framework on human rights is sufficiently suitable to guarantee freedom of expression before legal situations created by new technologies. Yet it has failed to specifically identify the need to regulate social media.

Carolyn Elefant, in her research The Power of Social Media: Legal issues and best practises for Utilities Engaging Social Media (2011) more specifically concentrate on wide use of social media and the need for its regulation. She defined social media a 'catch phrase that describes technology that facilitates interaction of information, user created content and collaboration. This paper describes the regulatory and legal issues potentially trigged by the use of social media. The author while discussing about best practises and social media policy accepts that banning of social media is not a social media policy. This study specifically focuses on traditional issues that businesses face when engaging in social media including Intellectual Property (IP) protection.

Many developing countries have now identified the need to regulate social media due to threats experienced on national security. Therefore, countries like Nigeria, Kenya and India have started to focus on regulation of social media.

E.Q. Okolie, in his research Extent of latitudes and limits of Social Media and Freedom of Expression within confines of Law in Nigeria (2019) elaborates on how social media erode away barriers and permit users to disseminate information effortlessly. While accepting the widening of the horizons of freedom of expression he states that 'wider spectrum provided for us to enjoy the freedom is not without limits.' Yet, he presents that 'uniqueness of social media poses certain challenges to law…'. The research arrives at the conclusion of – resulting the specific qualities of social media, existing laws alone is unable to regulate social media. For instance, the publishers on social media are not licensed journalists, they are merely exited people who wish to disseminate information. Therefore, the liberty to express oneself has clearly breached the requirement of fairness, reasonability and proportionality. This study very effectively presents the impact of social media on fundamental rights, consumer rights, and privacy but it has not addressed specifically impact of social media on national security. Currently attention need to be focused beyond protecting individual rights because social media has now begun to adversely affect public rights like national security.

In the research Assessing the Impact of Social Media on National Security in Kenya, D.P. Olasya (2016) has been able to identify the impact on social media on national security. He focuses on the use of social media to encourage terrorism, spread of propaganda, revolutionary activities, information leaking, financial fraud, spread of malware. The long-term terrorism experienced by Kenya has led to this study to recommend the need to regulate social media for the purpose of national security. In achieving such objective, the study determines specific strategies to curb and minimize the threats from social media to national security. He illustrates how existing cyber-crimes law has failed to regulate social media platforms (ex: vague terms like 'hate speech' does not entail what entails in it). The author ultimately shows the need for a separate legal mechanism to regulate social media. The study recommends for the establishment of a closed mechanism to monitor social media platforms and content published on social media. Although the author has highlighted the need for a separate mechanism to regulate social media, he has failed to focus on the means of achieving such end and the need to connect government, social media platforms and citizens is not seen (ex: vesting duty of care on social media platforms and making liability on intermediaries).

Even in Sri Lankan context studies have been conducted analysing expansion of cyber laws to address vast developing technologies. Due to the expansion of cyber laws, this concept was not a novel concept anymore. T. Abeysekara in his research 'A Game of Thrones': Law V

Technology: A critical study on the Computer Crimes Legislations in Sri Lanka identify the key areas of the Computer Crimes Act (CCA) which need to be revised and provide necessary recommendations to amend the existing laws in light of the technological advances. Further the study assesses the effectiveness of the act as a tool combating increasing criminal activities relating to information and communication technology. The author distinguishes between cybercrimes and computer crimes while re-defining several cyber related crimes which need to be recognised by CCA of Sri Lanka (like hacking, squatting, phishing). Further he interprets several terms in the act clearing certain ambiguities exist in the interpretation section.

Moreover, in the research Computer Crimes; Endless Race of Road Runner by the same author is an in-depth study on computer crimes regime in Sri Lanka. Cyber-crimes have been defined by referring to J. Clough. It states that 'computer crimes' is one of the number of terms used to describe the use of digital technologies in the commence and facilitate of a crime. Both the researches have recognised several offences which constitute computer crimes but studies are silent on the use of social media to threaten national security and the authority of the government to obstruct the use during an emergency. Due to the lack of separate provisions regulating social media, such need has to be covered by Section 6 of the CCA which include any action that danger national security, national economy and public order.

Therefore, a well evident gap exists in literature on the areas of social media, freedom of expression and national security in Sri Lanka. Resulting the risks created to national security by social media it can no longer be covered by the Section 6 of CCA. A mechanism beyond mere criminalizing or vesting delictual liability, connecting the government, social media platforms and citizens is needed to address the threats to national security. Therefore, this paper will address the gap existing in legislations regulating social media to combat threats created by social media.

III. DISCUSSION

A. SOCIAL MEDIA Defined.

The same rights people have offline must be protected online. As observed by Weeramanthry J., since the beginning of the industrial society little attention has been paid to a comprehensive analysis between technological innovations and implementation of human rights. This is highly related to Si Lanka. Due to the lack of law regulating social media, rights of the citizens have been crucially violated. Further, due to unregulated social media the national security is at a greater threat but unfortunately the only solution adhered was a limitless denial of access to social media. This clearly showcases the lack of proper mechanism to regulate social media even when the national security is at a threat.

Neither Computer Crimes Act (2007) nor Electronic Transaction Act (2006) of Sri Lanka provides a definition to 'social media'. Generally social media is a communication channel that transmit information to a wide audience and is usually a one-way street.

The Indian Ministry for the Electronics and Information Technology in their draft 'Framework and Guidelines for the use of social media for government organizations' states that social media can be broadly defined as any web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user content. It means social media covers a broader spectre. The gap lies in the development of the social media and legal framework shows that social media has gone beyond legal control.

B. Freedom of Expression via Social Media.

Primarily freedom of expression has been guaranteed by Article 14 (1) (a) of the Constitution of Sri Lanka where freedom of speech and expression including publication is guaranteed. In the frame of ICCPR and UDHR, freedom of expression is considered as "freedom to seek, receive, impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print in the form of art or through any other media of his choice". It is evident that the current international framework does not rule out the applicability of its regulation of new technologies. According to Balkin, the theoretical approach to the right of freedom of expression is aimed at creating a democratic culture. Therefore, freedom of expression represents as a main tool which allows more democratic participation. This right is interacting, which occurs in a way of communication among people who act as speakers and listeners.

The digital era, specifically through internet and social media has increased the choices of individuals and groups in full enjoyment of the freedom of expression. Nevertheless, unregulated use of media has exposed to unpredicted risks caused by the transition of these rights to the digital field.

Coccoli, has stated that same freedom of expression enhanced by new technologies is nowadays frequently frustrated by filtering, blocking and even disconnecting access. This led into a question whether today's regulatory framework of human rights is sufficient to guarantee the freedom of expression before legal situations created by new technologies.

C. Legal limitations on Freedom of Expression via social media.

Traditional freedom of expression guaranteed by the Constitution of Sri Lanka is restricted by the Article 15 (2) and 15 (7). Article 15 generally lays down the restrictions on fundamental rights. Article 15 (7) lays down a restriction upon Article 14 for the purpose of national security, public order, and protection of health and morality or respect the rights and freedom of others and for the general welfare. The right given has been totally taken away by this blanket restriction. Further, Article 15 (2) lays down a specific limitation on freedom of speech for the protection of racial and religious harmony.

By using these constitutional restrictions, the government has the capability to restrict the freedom of expression via social media.

Apart from that under Section 5 of the Public Security Ordinance No. 25 of 1947 the president has the power to make regulations (emergency regulations) for the interest of public security and for the preservation of public order. Therefore, the president is with the ability to restrict the use of social media.

These measures were taken by the government of Sri Lanka to regulate social media during several civil riots occurred in relation to the terrorist attack occurred on 21st April 2019 (Easter Sunday Attack). Racist opinions, fake news and religious criticisms were shared through social media leading the situation to its zenith. Immediately after the ban was lifted several websites were under cyberattacks including the Kuwait Embassy. Neither the Computer Emergency Readiness Team nor the Ministry of Digital Infrastructure and Information Technology were able to address this issue.

A problem arises as to whether the traditional restrictions on fundamental rights are compatible in addressing the issues created by the broadened freedom of expression in cyber space.

The Computer Crimes Act No. 24 of 2007 regulates the offences committed in cyber space. Section 6 of the act makes it an offence if any person who intentionally causes a computer to perform any function, knowing such will result in danger to national security, national economy, or pubic order. Publishing of any information via any social media platforms fall under the section since unavailability of any other law directly regulating use of social media.

In Sri Lanka the blocking of social media is done through Telecommunications Regulatory Commission (TRC) which was established by the Telecommunications (Amendment) Act No. 27 of 1996. Section 69 of the Telecommunication Act No. 25 of 1991 provides absolute power to the government to prohibit or to restrict the use of telecommunication at a time of public emergency or in the public emergency. Does social media fall within the ambit of telecommunication? 'Telecommunication' has been interpreted int Section 73 of the act, as "making of any transmission, emission or reception of signs, signals, wilting, images, sound or intelligence of any nature by optical means or by wire or radio waves or any other electromagnetic system.

Intellectual Property Act No. 36 of 2003 by Section 178(3) makes it an offence if any person knowingly and wilfully was in possession of has access to a computer program infringing the rights of the another and makes use of such programme for commercial gain. This section specially remedy an infringement of individual rights and it does not remedy an adverse effect on public rights like harmony and security. Further liability arises when a computer software has been used for commercial gain. Adverse actions without a commercial gain which affects national security cannot be covered under this right.

Similarly, common law remedies an infringement of individual rights in situation of defamation via social media by *actio injuriarum*. Damages for any harm for individual's dignity, reputation and integrity occurred through social media can be claimed by this remedy. Neither of these remedies address any harm done to national security via social media. Further due to complex nature of social media it is difficult to track down the actual or the original publisher.

Any existing legislations do not specifically address the regulation of social media. A regulatory mechanism should be created by connecting the government, citizens and the social media platforms to ensure national security. Social media platforms should be responsible for the information shared via their platforms and a duty of care should be vested on them. If such precautions are not followed by the specific platform the government should have the ability to ban such social media platforms from the country since it can be a threat to national security. Yet banning has not been accepted as a balanced legal approach. It amounts to violation of freedom of speech and expression.

Resulting internal cohesion created through social media in Sri Lanka constantly in the years of 2018 to 2019, proved that the existing legal framework is incapable of addressing legal, policy and regulatory aspect of the use of social media in Sri Lanka. This has caused legitimate concerns over curtailing constitutional guarantees of freedom of speech and expression.

D. To strike a balance between National Security and Freedom of Expression: Learning from India.

A problem arises to any rational mind 'is banning the required solution?' Or 'is it merely a slippery slope due to the lack of legal framework to regulate social media?'.

Unlike Sri Lanka many other countries like Unites States, United Kingdom, South Africa and India owns a broad legal framework addressing many challenges faced due to electronic communication including social media. Recent incidents provide proof that Sri Lanka is not sufficiently equipped to handle social media during an internal disturbance. A law beyond traditional fundamental rights guarantees and limitations need to be adhered.

In contrast to Sri Lanka, India owns an expanded legal framework in relation to managing technology and communication. Moreover, having shared similar social and cultural issues (protest over Delhi gang rape in 2012, Assam riot in 2012, Mussafarnagar riot in 2013), India provides most relevant and appropriate remedies to Sri Lanka to build up a well-regulated legal mechanism to monitor social media in achieving peace and stability. Therefore, Indian Information Technology Act No. 21 of 2000 (IT Act) and its latest amendment of 2008 set an example to Sri Lanka.

1.Sending offensive messages and cyber terrorism: Section 66 of the act recognises computer related crimes and Section 66A deals with the offence of sending offensive messages through communication services. It states that "any person who sends by means of a computer resource or a communication device (a)any information that is grossly offensive or has menacing character or (b) any information which he knows to be false but for the purpose of annoyance, inconvenience, danger, obstruction, insult, injury, Criminal intimidation, enmity, hatred…". This can be used to arrest people for publication of opinions on social media which is a risk for security and stability. Further, Section 66F defines cyber terrorism and makes it an offence. It includes whoever threatens the unity, integrity, security or sovereignty of India by obtaining access to information, data that is restricted for the purpose of national security and obtained for the purpose of causing injury to the interest of sovereignty and integrity of India.

These sections (66A and 66F) addresses the emerging issues in cyber space. Although still Sri Lanka has not experienced cyber terrorism such law will strengthen national security and minimize the threat.

2.Regulate Arbitrary banning and denying access: The IT Act of India provides a mechanism to prevent arbitrary banning social media. Section 69A provides power to issue directions for blocking for public access of any information through computer resource. Rules under Section 69A (rule 7) authorises the Secretary, as a competent authority to issue directions for blocking of information for public access after examining recommendations of a committee comprising of designated officer, joint secretaries of Ministry of Home Affairs (MHA), Ministry of law and Justice and Information and Broadcasting and Indian Computer Emergency Response Team (ICERT). And rules required the committee to examine the request within 48hours and later a Review Committee chaired by Cabinet Secretary review the decision taken by the competent authority for blocking information for public purpose.

Cyber experts view that blocking of information is ineffective as a result of the use of Virtual Private Networks (VPN) which enables to hide someone's location by funnelling data through a server in another country. Furthering banning and blocking need to be less arbitrary and more transparent. It is well evident that India owns a well-regulated and supervised mechanism for blocking information for national security and public order.

It is very crucial that even Sri Lanka adopt such procedure before banning or blocking access to information because it directly takes away freedom of expression of the citizens. Any act of government specially at a time of national discrepancy should not be arbitrary. Pranesh Prakash, in commenting on blocking of access to information, states "informing censored groups/individual reasons for the block and allowing them to contest it and seek redress from the relevant authorities, encourages openness". This will certainly pave the way in balancing national security and rights of the citizens.

3. Duty on intermediaries: Section 79 of the Indian IT Act vests a duty towards the intermediaries (internet service providers - ISP) making them responsible for the information which they make available to the users. Internet intermediaries refers to the companies that facilitate the use of internet. Such companies include ISP, search engines and social media platforms.

Section 67C provide for the preservation and retention of information by intermediaries when prescribed by the government and the intermediary has made liable for any failure to follow or contravenes such direction.

Section 79 provides only for a limited exemption from liability of the intermediaries. The liability is vested in situations where intermediary initiate the transmission, select the receiver of the transmission and select or modify information contained in the transmission. This immunity for the intermediaries will not arise in situations where it fails to remove, disable access to such information. It is evident that under Indian law intermediaries does not go unregulated. They owe certain code of conduct vesting liability in specific situations.

It requires the intermediaries to observe due diligence while discharging their duties and upon receiving knowledge that any information controlled by such intermediary is being used to commit an unlawful act, the

intermediary should remove or disable access to that material. Inclusion of such section vests responsibility over social media platforms to be responsible for the information shared through them. This will tend to minimize the misuse of information through social media.

This vests a shared responsibility over the government and the service providers. This is a new paradigm in regulation which is referred as co-regulation.

E. Direction for future internet regulation: Learning from UK.

Unlike India, many western countries have initiated in drafting septate regulatory mechanisms to combat the threat from social media for the national security. Some have recommended fining systems-imposed on the social media companies and imprisonment of social media executives if they were unable to remove the violent content from social media. Rather than moving to such a strict mechanism, a proper regulatory body to monitor the social media platforms is required.

Very recently (on 8th April 2019) the government of UK along with their Department for Digital, Culture, Media and Sport, Home Office introduced a proposal for world's first online safety laws.

This proposal which was referred to as the 'Online Harms White Paper' was introduced with the objective of addressing a range of online material, including the threats to national security (ex: cyber terrorism and spread of hate speech)

Although this was criticised as a historic attack on freedom of speech and free press, it provides new mechanisms of regulating social media by connecting the government, social media companies and individuals. Even the online companies said they support the idea of ensuring safer internet. This new code of UK certainly provides Sri Lanka with certain recommendations in regulating social media to achieve a sustainable balance between national security and rights of the citizens. Therefore, this paper will focus on certain lessons which Sri Lanka can adopt from UK proposal for the effective regulation of social media in order to strengthen national security.

1.New Regulatory Model: Through this regulatory model, the government has proposed a new statutory duty of care to make companies to take more responsibility in tackling with the harm caused by its content. The compliance of the duty of care will be over seen and enforced by a separate independent regulator. All companies need to be capable to show that they are fulfilling their duty of care. In breach of duty of care the regulator will have the power to issue substantial fines and impose liability to senior officers of the management.

Further, new regulatory model intends to develop a new culture of transparency, trust and accountability. Annual reports outlining the prevalence of harmful content on their platforms and what counter measures they are taking to address them will be regularly demanded. The regulator has the power to publish them online, so that users can be well informed. Importantly, the regulator has the power to require additional information on any emerging threat.

This above-mentioned statutory duty of care requires the companies to take responsible steps to keep users safe and prevent other persons coming to harm. Companies must fulfil its statutory duties and regulator will set out what to do in a code of practise. The companies will strictly have to stick into the code and the governments will have the power to guide the regulator in relation to code of conduct relating to terrorist activity which risk national security.

Such regulatory model can be adhered in Sri Lanka in developing a proper legal mechanism to monitor social media. Mainly by vesting a duty of care on the intermediaries of the social media companies, the social media will be well monitored and the flow of information will be clearly observed. This will lead to exercise of safe and well-regulated freedom of expression through social media which will enhance public security.

2.Independent Regulation: An independent group of experts with knowledge on information technology, law, administration and research need to be appointed in order to execute this regulatory model. It will implement, oversee and enforce exercise of duty of care by the companies. It needs to be comprised of experts with right expertise knowledge and capabilities to perform their task. In order to execute their power necessary labs, research and technological teams need to be established. In Sri Lanka the obstacle of technological literacy and lack of technological facilities need to be overcome.

This independent group is expected to promote education and awareness about online usage, specially at a time of emergency risking national security. This board should encourage development and adoption of safe technologies to tackle online harms.

Sri Lanka necessarily have expertise knowledge on the field of information technology and law. A body connecting these separate fields need to be created because no longer technology and law cannot stay in isolation. Such body need to be provided with required resources, facilities and technology. Further, such regulatory body need to be an independent and politically independent group because it abridges users, government and technology.

3. Using Technology as a Solution: Online Harm White Paper suggests that technology itself can be used as a part of the society. Technology can play a crucial role in keeping users safe online. It suggests that by designing safer and more secure online products and services, the technological sector can equip all companies and users with better tools to tackle online harms. The proposal is headed with the objective of making UK to be world leader in the development of online safety technology and to secure companies of all sizes to have access and to adopt, innovative solutions to improve the safety of their users. This includes introducing new safety software to filter inappropriate information and introduction of safety apps.

Due to the existing economic situation of the country, initiating such massive projects which require a vast capital and technological knowledge seems to be impractical. Therefore, at initial stage the government can initiate in implementing small scale projects to elevate the technological innovations.

III. RECOMMENDATIONS

Sri Lanka can move for a sperate pro-active regulatory mechanism to regulate social media. A collaboration between government and social media platforms is needed. (ex: Online Falsehood Bill of Singapore, UK Online Harm White Paper)

Vesting liability on intermediaries established in Sri Lanka for the content harming national security following Manila Principles on Intermediary Liability (ex: Section 67 and 79 of Indian IT Act). Further, Sri Lanka can shift to 'intermediary responsibility' from 'intermediary liability'.

Establishment of an independent committee including experts on information technology, law and research to monitor social media. This committee will interconnect government with social media platforms. Then neither the government nor social media platforms will have total authority over social media.

Extension of existing cyber laws in Sri Lanka to include unaddressed aspects like denying access and banning for national security, cyber terrorism. Cyber laws should be expanded beyond protection of individual rights to public rights.

Using social media as a solution rather than a problem. Initiate propagandas for improving awareness on the use and harm of social media through social media itself. Provide educational and technical and financial assistance to youth for new safe technical innovations. (ex: building filtering software)

III. CONCLUSION.

Ensuring freedom of expression via social media during an emergency, while assuring national security seems unrealistic. Yet, through co-regulation, the government and social media platforms can work together collaboratively to have joint responsibility and accountability for regulation of social media. Such shared responsibility in the cyber space will lead to online safety while enhancing free flow of information via social media. Social media brings tremendous public value such as freedom of expression. However, it has enabled individuals to spread hate speech, terrorists' agendas and spread of fake contents which can threaten national security. Even in media space, government is regarded as the guardian of public interest. Therefore, rather than moving to a drastic and extremist end, the government should own a mechanism to regulate social media in a well-disciplined way.

List of References.

Abeysekara T. and Elkaduwa S. (2015) A Game of Thrones': Law V Technology: A Critical Study on the Computer Crimes Legislations in Sri Lanka, *International Conference on Interdicilplinary Legal Studies.*

Abeysekara T. (2015) Computer Crimes; Endless Race of Road Runners', *JSA Law Journal,* volume 3, page 127.

Aswad, E.M. (2018-2019) The Future of Freedom of Expression Online, *Duke Law and Technology Review.*

Bakircioglu, O. (2008) Freedom of Expression and Hate Speech, *Tulsa Journal of Company and International Law,* volume 16, page 1.

Coccoli, J. (2017) The Challenges of New Technologies in the Implementation of Human Rights: An Analysis of Some Critical Issues in the Digital Era*, Peace and Human Rights Governance*, volume 1, page 223-250.

Donnerstein, E. (1994) Mass Media Violence: Thoughts of the Debate, *Hofstra Law Review,* volume 22, page 827.

Elefant, C. (2011) The Power of Social Media: Legal Issues and Best Practises for Utilise Engaging Social Media*, Energy Law Journal*, volume 1.

Joseph, S. (2012) Social Media, Political Change, and Human Rights, *B. C. International and Company Law Review*, volume 35, page 145.

Okolie, E.Q. (2019) Extent of the Latitudes and Limits of the Social Media and Freedom of Expression within the confines of Law in Nigeria, *Journal of Law, Policy and Globalization,* volume 83, page 162.

Olaya D.P. (2018) Assessing the Impact of Social Media on National Security in Kenya, page 24.

Novek, C. (2017) Rights-Based and Tech-Driven: Open Data, Freedom of Information and Future of Government Transparency, *Yale Human Rights and Development Law Journal,* volume 1.

Pandal, S. (2016) *The 'Social Media' Challenge to National Security: Impact and Opportunities.* 1st Edn. New Delhi: Institute of Defence studies and Analysis.

Pavlovic, M. (2017) Legal Limitations of Freedom of Expression in Media, *International Journal on Economics and Law,* volume 7, page 33.