Regulating Cyber Communication: A Global Human Rights and Law Enforcement Challenge[1]

Murdoch Watney
University of Johannesburg
Faculty of Law and Department of Public Law
Johannesburg
South Africa
e-mail: mwatney@uj.ac.za

Abstract

The right to free speech and privacy on the Internet enjoy protection as human rights. However, there may be instances when the right to free speech or the right to privacy pertaining to cyber communication may be limited for criminal law and national security enforcement. It is important to establish in which circumstances the limitation of free speech and/or privacy will be justifiable. Once established, it should be considered how Internet regulation may be accomplished. As a user cannot gain access to the Internet or transmit, host or store communication without an intermediary, the intermediary will have to assist and co-operate with cyber communication regulation. Should regulation be imposed on the Internet intermediary by means of liability in the format of legislation and/or should an intermediary have a responsibility for self-regulation of content? If free speech or privacy is limited in circumstances that do not qualify as necessary and proportionate, which recourse does a user have? Similarly, may an intermediary refuse compliance with a request from law enforcement? Globally governments face the challenge of regulating cyber communication for the purpose of law enforcement within the context of human rights protection.

Keywords: *cyber communication; legal regulation; human rights protection; law enforcement; intermediary*

---

1. Introduction

The way people communicate today has drastically changed from the manner in which their ancestors communicated. Face-to-face communications have made way for faceless, cross-border and interactive many-to-many communication. Mobile phones and the Internet have become an integral part of most people's lives and define the manner in which many people communicate. People do not only connect to the Internet by means of computers but increasingly use mobile phones to connect to the Internet, send WhatsApp or Twitter messages, take photos and/or record videos which they then upload onto social media sites. People make

[1] The financial assistance of the NRF (UID 85384) is hereby acknowledged. Opinions expressed are those of the author.

comments and express opinions on articles and post blogs that interest them. It is therefore not surprising that today is referred to as an "information age" in which access to information and participation in the exchange of information is a distinctive characteristic of the global world.[2]

Cyber communication whether verbal or in the format of words or visual in the format of videos, music and pictures may be abused for various illegal purposes, such as cyber bullying, revenge pornography and hate speech to name but a few. Governments have a legal duty to protect nationals against such communication and in some instances to protect nationals against themselves from exploiting the right to communicate online.

Governments and/or users are concerned not only about the manner in which cyber communication may be abused but also about the content of communication. Users are justifiably concerned that their right to free speech may be limited in circumstances where a government perceives their communication as a threat and tries to suppress their communication on the Internet.

The discussion focuses on which cyber communication may be considered unlawful, how a government may regulate illegal communication and the impact regulating cyber communication may have on human rights protection specifically the right to free speech and to a limited extent, the right to privacy inherent to free speech. Although hate speech and incitement to hate and acts of terror pose an ever-continuing threat and danger to governments and users on a global level, the discussion will not focus only on such communication.

The aim of this discussion is not to criticize a government for the manner in which it has elected to regulate cyber communication but to reflect on whether such regulation is necessary and proportionate within the context of human rights protection balanced against criminal and national security law enforcement. A government that unjustifiably restrict cyber communication should re-consider the limitation and restore the imbalance created by the unjust state interference pertaining to the cyber communication. As will be illustrated hereafter, governments on a global level face legal challenges pertaining to cyber communication regulation which necessitate discussion.

2. Legal Challenges pertaining to Cyber Communication Regulation

Communication on the Internet differ from the physical world in many aspects due to the characteristics of the Internet. The Internet has opened up many modes of communication and

[2] Laidlaw *Regulating Speech in Cyberspace* (2015) 9; Lederman *Infocrime* (2016) 15 – 16.

although cyber communication has many benefits, it also poses many risks and threats which are not only experienced on a national but also on a global level.

Internet users tend to be disinhibited in what they do and/or say in cyberspace.[3] Consider the legal position where a married woman by accident sent a picture of herself which was sexually comprising and intended only for her husband to a school hockey WhatsApp group comprising of 17 members.[4] The woman immediately realised her mistake and apologised to the members of the WhatsApp group. She was completely oblivious that some members of the WhatsApp group forwarded the sexually comprising picture to other non-members and also posted it on the Internet.[5] Dissemination on different platforms is a characteristic of the Internet and it can persist for long time unless deliberately removed.[6] Does the forwarding and/or postings of the image without the consent of the woman constitute unlawful cyber communication? Maybe an argument could be made that cyber communication is not private, that the woman did not have a reasonable expectation of privacy once she made use of WhatsApp and that by exercising her right to freedom of expression, she must accept the consequences of exercising such speech.

Contrast above situation with the example of Justine Sacco who on 20 December 2013 prior to her departure from London to South Africa tweeted to her 170 followers the following "Going to Africa. Hope I don't get AIDS. Just kidding. I'm white".[7] Her comments were not well-received and offended many. Although her tweet was not illegal and merely misguided, she was condemned and disgraced on social media platforms and suffered reputational damage. Sacco deleted her Twitter account but her comment had already been disseminated worldwide.[8] Once disseminated, it is very difficult to ensure a stay-down as cyber communication is inherently cross-border.

Comments made in the passing and which in a pre-Internet age would not have elicited much attention, are now exacerbated if the same comments are made on the Internet. *Chambers v Director of Public Prosecutions* [2012] EWHC 2157, the so-called "Twitter Joke" case

---

[3] Harvey *Collisions in the digital paradigm* (2017) 38; Stauffer "The Internet is not the enemy", available at https://www.hrw.org/world-report/2017/country-chapters/the-internet-is-not-the-enemy.
[4] Pillay "SA looks to criminalise revenge porn" available at http://www.timeslive.co.za/scitech/201608/30/SA-looks-to-criminalise-revenge-porn.
[5] Pillay (n 4).
[6] Stauffer (n 3).
[7] Harvey (n 3) 271 272.
[8] Harvey (n 3) 310.

illustrates how cyber communication may be misinterpreted.[9] At the end of 2009 and beginning of 2010 the United Kingdom (UK) experienced very bad weather conditions with the consequence that some airports had to be closed. Mr Chambers who was about to travel from the Robin Hood airport send a Twitter message to his 600 followers to the effect that if the airport was closed due to bad weather that he would blow up the airport. Law enforcement did not take his Twitter comment lightly and he was arrested, charged and convicted for sending a menacing message. The High Court overturned his conviction in 2012.[10] The positive outcome of this case was the implementation of interim guidelines in respect of prosecuting cases involving communication sent via social media.[11]

There are many examples of the exploitation of Internet services. For example, Facebook implemented "Facebook Live" at the end of December 2015 for the purpose of streaming life from a mobile phone to Facebook harmless videos such as the user being at the beach or attending a concert.[12] Unfortunately, "Facebook Live" has been abused for purposes other than what it was intended for, such as police brutality, sexual assault, suicide and murder. In April 2017 the Internet community was shocked by the life broadcasting of two video clips on "Facebook Live" of a Thai man killing his 11-month daughter. The man filmed the murder of his daughter on the rooftop of a deserted hotel on his mobile phone and streamed the video clips to "Facebook Live". The video clips were accessible to users on his Facebook page for approximately 24 hours before take down.[13] Do these types of cyber communication mean that "Facebook Life" should be banned, or alternatively does the intermediary have a responsibility to self-regulate content and to take precautionary measures to pro-actively prevent this type of communication? If affirmative, how will the intermediary ensure that this type of communication abuse does not occur?

Physical acts of terrorism affect all countries. Governments worldwide face the immense task of preventing such acts of terror by obtaining intelligence prior to such attacks to prevent it from happening. It is an indisputable fact that social media sites are specifically targeted to spread propaganda, incite others to hate and committing acts of terror. It is alleged that ISIS is the most successful terrorist organisation in history using the Internet for distributing its

---

[9] Harvey (n 3) 266, 268.
[10] Coleman "Robin Hood Airport tweet bomb joke man wins case" available at http://www.bbc.com/network/news/uk-england-19009344 .
[11] Harvey (n 3) 272 – 273.
[12] Gibbs "Facebook under pressure after man livestreams killing of his daughter" available at https://www.theguardian.com/technology/2017/apr/25/facebook-thailand-man-livestreams-killing-daughter.
[13] Gibbs (n 12).

propaganda, dissemination of its news and more importantly to communicate.[14] It was revealed that prior to the 2017 terrorist attack at the Reina club, Istanbul, Turkey, the perpetrator communicated on his mobile phone by means of Telegram.[15] Telegram has allegedly become one of the main communication devices of ISIS with the consequence that Europol, the European policing body, has condemned Telegram for failing to join the fight against terrorism.[16] Since 2014 most social media intermediaries have taken a strong stand in the implementation of take-down policies pertaining to ISIS whereas Telegram has allegedly not followed the same approach.[17]

The issue of encryption gained a lot of attention in the aftermath of the 2015 San Bernardino terrorist attack. Many governments have indicated that they want access to encrypted communication.[18] WhatsApp as well as Telegram employ end-to-end encryption which locks law enforcement out of the communication. In the 2017 United Kingdom (UK) Westminster attack, the perpetrator, Masood, was on WhatsApp minutes before ploughing into dozens of pedestrians and stabbing a policeman to death at the gates of the parliament.[19] In the 2015 San Bernardino killing the police requested Apple to provide access to the perpetrator's encrypted communication on his iPhone. Apple indicated that it did not have access to the communication and that re-designing the security feature would compromise all iPhone users' security and privacy. Although law enforcement indicated in 2016 that it did not need assistance from Apple, the issue of access to encrypted communication is far from being settled.[20] Should law enforcement gain access to such encrypted communications in the interest of national security or would it violate the human rights to privacy and security of all users? In this instance decryption does not violate the right to free speech but it may violate the right to privacy and cyber security protection inherent to exercising free speech.

Some countries may take legal action in circumstances where the cyber communication is considered offensive to the culture, traditions and customs of a specific state. Cyber communication may be deemed insulting to a specific person who holds a special office, namely a country's present or former monarch or president. In this regard, the Thailand

[14] Ahmet and Speckhard "Telegram: the mighty application that ISIS loves" available at http://www.icsve.org.
[15] Ahmet and Speckhard (n 14).
[16] Ahmed and Speckhard (n 14).
[17] Ahmed and Speckhard (n 14).
[18] Watney "Law Enforcement Access to Password Protected and/or Encrypted Mobile Data" presented at 2016 11th International Conference on Availability, Reliability and Security.
[19] Tapsfield "This terrorism sent a WhatsApp message and it can't be accessed" available at http://www.dailymail.co.uk/news/article-4350264/Rudd-demands-access-encrypted-WhatsApp-messages.html
[20] Watney (n 19).

government indicated that they will prosecute anyone who looks at online material deemed insulting to its monarchy. Article 112 of Thailand's Criminal Code B.E. 2499 of 1956 provides that anyone who insults the monarchy commits a crime and may be punished with a prison sentence up to 15 years.[21] How will law enforcement establish whether a Thai national watched cyber communication deemed insulting to the monarchy and/or where users indicated that they liked the post or shared it with others? In the latter instance, the intermediary will have to provide the information. Should social media intermediaries provide such information and if affirmative, would it not amount to a violation of the right to privacy? In 2017 the United Nations (UN) Human Rights Committee found that all people have the right to criticize public figures as it forms part of freedom of expression and advised Thailand to re-evaluate their Criminal Code.[22] If a government elects not to re-visit a cyber communication limitation, is there any recourse to force such a government to adhere to a recommendation?

A state subjected to protests may be predisposed to blocking access to social media sites and/or the Internet in the interest of public welfare and national security. Turkey for example blocked access to social media sites such as Facebook and Twitter in the aftermath of the 2016 militant attacks.[23] In 2017 access to Wikipedia was blocked for providing access to an article and comments alleging that Turkey was involved in terrorist organisations.[24] Wikipedia allegedly refused to remove the article with the consequence that the Turkish government deemed it in the interest of national security to block access to the website.[25] Should a state be criticized for blocking access to the Internet to prevent the spread of propaganda against a government which may result in instability within a country? The latter question may be considered against the background of the "Arab Spring".

The revival of state control over the Internet originates in part from the events in the Middle East which became known as the "Arab Spring".[26] The "Arab Spring" refers to anti-government protests that spread across the Middle East early 2011. The protests were characterized by extensive use of social media such as Twitter to organize and spread

---

[21] Abkar "Thailand to prosecute anyone that even looks at material considered insulting to the monarchy" available at www.dailymail.co.uk/.../Thailand-prosecute-internet-insult-monarchy-king-crop-top.ht.
[22] "UN very concerned on *lese majeste*" available at https://thaipoliticaprisoners.worldpress.com/tag/article-112.
[23] Phippen "Why Turkey blocked Access to Wikipedia" available on http://www.theatlantic.com/news/archive/2017/04/turkey-blocks-wikipedia/524859.
[24] Phippen (n 23); Lowen "Turkish authorities block Wikipedia without giving a reason" available on http://www.bbc.com//news/world-europe-39754909.
[25] Phippen (n 23).
[26] Harvey [n 3] 94.

awareness.[27] Governments perceived the use of social media during the "Arab Spring" as a threat which resulted in access to social media being blocked. Does a national have an absolute right to free speech and/or access to the Internet or does a government have the right to limit such a right and if affirmative, in which circumstances may such a right be limited?

Over the years South Africa has experienced xenophobic attacks. Prior to the attacks, many posts on social media sites expressed hate and incitement of violence towards foreigners.[28] These posts are unlawful and pose a threat to all people. In this regard, the role of the intermediary in preventing and/or detecting such posts should be investigated. Should such posts be removed and/or access to it blocked or would it amount to the application of censorship?

In April 2017 the South African government cautioned South Africans on its official Twitter account not to use social media in a way that could be harmful to the image of South Africa.[29] The South African government indicated that it may consider regulating social media but the form of regulation was not outlined. Will the government expect social media intermediaries to pro-actively monitor communication and to remove and/or block communication that reflect negatively on South Africa's image such as criticism against government corruption? How will such regulation impact on freedom of expression and which safeguards will be in place to protect a user in circumstances where lawful cyber communication was blocked or removed?

Above examples illustrates the legal challenges confronting countries pertaining to cyber communication regulation. Does a user have human rights regarding cyber communication and if affirmative, are these rights absolute or may it be limited for criminal law and national security enforcement? If such rights may be limited, in which circumstances will such a limitation be justifiable?

3. A Synopsis of the Existence of Human Rights on the Internet

The right to free speech and privacy on the Internet are recognized as human rights. Article 19 of the Universal Declaration of Human Rights (UDHR) of 1948 provides for a right to freedom of expression. The International Covenant on Civil and Political Rights of 1966

---

[27] Harvey [n 3] 94.

[28] Davis "Pandora's Box: South Africa and the (mis)use of social media" available at https://www.dailymaverick.co.za/article/2017-04-05-pandoras-box-south-afica-and-the-misuse-of-social-media/WT_US60w00o

[29] Davis [n 28].

uses similar language. The right to freedom of expression is also protected in article 10 of the European Convention on Human Rights (ECHR) of 1950. The right to privacy is protected in article 12 of the UDHR and article 8 of the ECHR.

In July 2016 the UN Human Rights Council adopted a non-binding Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet. The UN Human Rights Council's resolution specifically condemns measures to prevent or disrupt access to the Internet and calls on all states to refrain from and cease such measures. It also recognises the importance of access to information, privacy online for the realisation of the right to freedom of expression and to hold opinions without interference. The Resolution provides guidelines to participating states on how governments should shape laws when it comes to free speech and access to information on the Internet.[30] It may be argued that a government cannot limit the right to access in order to suppress dissidents or activism against a government to ensure it stays in power.

Stauffer[31] discusses the limitation of human rights. Where a state limits the right to free speech or privacy, it must demonstrate that such a limitation is necessary by showing that there is a direct and immediate connection between the right to be restricted and the threat. It must also show that the limitation is proportionate in other words that the limitation is the least restrictive means to protect the public interest.

The right to free speech and privacy are not absolute rights. Stauffer [32] correctly indicates that in some instances restrictions to the right of free speech are essential to protect people from terrorism, incitement to violence and revenge pornography. Free speech does not encompass child pornography and images that may be harmful to the protection of minors. It is therefore important to establish the manner in which unlawful cyber communication should be regulated.

4. Regulation of Cyber Communication

Law enforcement in general does not have direct access to communication on the Internet. As some form of intermediary are always involved in cyber communication, an Internet intermediary is in the ideal position to regulate conduct and communication on the Internet. Regulation may be imposed by means of liability (legislative regulation) or by means of a responsibility for content (self-regulation). In some instances, a court judgment may

[30] Velocci "Internet Access is now a basic human right" available at http://gizmodo.com/internet-access-is-now-a-basic-human-right-1783081865.
[31] Stauffer [n 3].
[32] Stauffer [n 3].

impose a liability such as the "right to be forgotten"[33] which will be referred to hereafter at paragraph 4. This liability is now provided for in the European Union (EU) General Regulation on Data Protection (GDPR 2016/679).

Governments worldwide struggle with cyber security. In this regard the EU must be applauded for addressing various cyber issues. In many instances the EU approach has become the standardized approach for other non-EU countries. It is therefore important that whichever solution to cyber security the EU implement, the consequences and impact of such a decision is carefully scrutinized.

The Council of the European Union is at present looking at ways on improving criminal justice in cyberspace. The Council has identified 3 areas that need to be improved, such as assistance and co-operation between law enforcement and intermediaries; access to information stored outside the borders of a country and jurisdiction.[34] As regulation of the criminal justice in cyberspace affect all countries, it would be beneficial if countries on an international level could come to some agreement on a harmonized approach in addressing the concerns identified by the Council of Europe.[35]

The Council of Europe Convention on Cyber Crime of 2001, also referred to as the Budapest Convention, promotes the importance of mutual assistance, international cooperation and adopting a common criminal policy. Chambers-Jones[36] indicates that although the convention must be commended, the convention is out of date. It was not drafted against the background of terrorism and predominantly regulates illegal conduct. Today regulation must include communication regulation. The Budapest Convention is also not an international agreement but a multi-national agreement and some may perceive it as an instrument of the European Union. It would be useful if a cybercrime convention regulating conduct and communication could be drafted under the auspices of the UN on international level.

At present the biggest challenge lies in terrorist-related communication where social media is abused for spreading propaganda and inciting others to commit acts of terror. How must the intermediary deal with such communication? The European Commission made in 2016 proposals under the Digital Single Market initiative that target specifically Internet

---

[33] Laidlaw [n 2] 186 – 187; Harvey [n 3] 298 – 304; Stauffer [n 3].

[34] Council of Europe "Progress Report following the conclusion of the Council of the European Union on Improving Criminal Justice in Cyberspace" available at https://db.eurocrim.org/db/en/vorgang/342/

[35] (n 34).

[36] Chambers-Jones *Virtual Economics and financial crimes* (2012) 202.

intermediaries.[37] Internet intermediaries will have a responsibility for self-regulating communication and specifically the content. The responsibility for self-regulation cover three areas, namely terrorism, hate speech and protection of minors. Self-regulation means that an intermediary must pro-actively monitor all communication to identify speech that amount to terrorism or hate speech or may have a negative impact on minors. Once identified, the intermediary must take down or block access to the communication.

There are various concerns with the imposition of self-regulation on the intermediary. These concerns relate to the imposition of a general obligation to monitor, a stay down request, over-blocking and liability for taking down lawful content or not removing unlawful content.

Article 15 of the E-Commerce 2000/31/EC provides that an intermediary does not have a general obligation to monitor. The latter principle was illustrated in the case of *SABAM v Netlog Nv*, Case C-360/10 where the European Court of Justice (ECJ) determined that a hosting service provider could not be obligated to impose a general filtering system for an indefinite period of time of the data of all users.[38]

A stay down request that information that has been removed or blocked must stay down permanently would be difficult to achieve. Stay down refers to circumstances where an intermediary must ensure that once a file has been removed, it will not re-appear on the system, such as terrorist-related communication. To ensure a stay down, the intermediary will have to make use of content scanning or filtering.

Another valid concern is that self-regulation may result in over-blocking. Horton[39]indicates that the decision to take down will be based on database matches and computer algorithms and not on the human understanding of the law. For example, websites that had no connection with pornography such as the Owl and the Pussycat Center in Scotland which is a nature reserve offering children's adventure activities and Struthers London, a specialist luxury watch-making business, were blocked.[40] Intermediaries are cautious when receiving a take-down or blocking request and will remove or block content as a precautionary measure. There should be a speedy method for redress for the owner of a website which has

[37] Horten "The looming cloud of uncertainty for Internet intermediaries" available at http://www.cdt.org.
[38] Horten [n 37]; Laidlaw [n 2] 121.
[39] Horten [n 37].
[40] Horten [n 37].

been blocked unlawfully but at present it appears that websites that have been blocked, have little, if any recourse for unblocking it.[41]

It is important to establish whether an intermediary may be held liable for taking down a website that was lawful. Intermediaries in the instance of self-regulation exercises their own discretion. Intermediaries are corporate bodies and not a public or judicial body. In most instances, the take down is not done by means of a judicial order. Intermediaries may therefore be targeted for not removing content that are deemed offensive or for removing content in violation of freedom of expression. The EU intermediaries position is not as certain as the position of United States (US) intermediaries where intermediaries enjoy a high level of protection.[42] Section 230 of the Communications Decency Act (CDA) 47 U.S.C of 1996 (CDA) provides that intermediaries cannot be treated as a publisher or a speaker where content is posted on their systems. Section 230 also includes a double safety net in a 'Good Samaritan' clause which provides that where they take down content which they believe in good faith to be obscene, violent etc., they cannot be held liable.

There are instances when an intermediary may be exempted from liability for third party user-generated content, such as defamatory, obscene content, terrorism and content which stirs up religious or racial hatred.[43] Article 12 – 15 of the E-Commerce regulate intermediary liability exemptions. Horten[44] distinguishes between network intermediaries and hosting intermediaries. Hosting intermediaries will be protected against liability if they expeditiously remove illegal content when they are provided with actual knowledge that it exists on their site, server or system. A search engine may be requested to remove a link to third party user-generated content that is not unlawful but where such content is not adequate, irrelevant or not relevant any more. This latter principle referred to as the "right to be forgotten" was outlined in the *Google Spain* case.[45]

Self-regulation as proposed by the European Commission regarding a Digital Single Market may result in legal uncertainty. Horten[46] correctly indicates that countries may have a different approach to removal. For example, in Germany images of swastikas may be considered hate speech but in another country such as the US it would form part of free speech.

[41] Horten [n 37].
[42] Horten [n 37].
[43] Laidlaw [n 2] 125.
[44] Horten [n 37].
[45] Laidlaw [n 2] 186 – 187; Harvey [n 3] 298 – 304; Stauffer [n 3].
[46] Horten [n 37].

Likewise, a painting that may be considered fine art in one country and therefore legal, may be perceived as sexually offensive in another country and may be removed. It is proposed that communication regulation should be imposed by means of liabilities outlined in legislation which provides for intermediary protection and review procedures. Such legislation will ensure legal certainty to intermediaries providing services to different countries.

Intermediaries face many challenges in respect of illegal communication. As indicated "Facebook Live" and other life-streaming services may be abused. Intermediaries have terms and conditions outlining which communication would be unlawful. However, these terms and conditions do not always deter unlawfulness. Intermediaries should remove offending videos as soon as possible.[47] It may be that live-streaming services should employ their own monitors and not rely only on automated means or flagging of content. If social media intermediaries do not take down offending content, then legislation must provide for intermediary liability. Merely relying on self-regulation will not be successful if there is no enforcement mechanism.

The issue of state interference with cyber communication warrants consideration. Does a user have some form of recourse in circumstances where a user's right to free speech or right to privacy inherent to free speech was limited? May an intermediary refuse compliance with a request from law enforcement for access to and/or information regarding cyber communication?

5. Remedies for State Interference with Cyber Communication

If an intermediary receives a request from law enforcement, then an intermediary may refuse compliance but the non-compliance must be subjected to a review by a court. The intermediary cannot merely refuse compliance without the justifiability of the non-compliance being scrutinized.[48] An intermediary is not merely an extension of the state for purposes of surveillance such as monitoring but has a responsibility to protect the rights of customers against a request from government which seriously violates human rights. A good example is the *SABAM v Netlog* case referred to earlier at paragraph 4.

A user should be provided recourse regarding state interference with cyber communication. As indicated earlier, if a legal communication is blocked or removed, the user

[47] Gibbs [n 12].
[48] Bilchitz "Privacy, surveillance and the duties of corporations" 2016 *South African Law Journal* 66.

should be provided with a remedy to re-institute the communication. This is a legal issue that necessitate serious consideration.

In *Ahmet Yildirim v Turkey* Application no. 3111/10 (18 December 2012), Yildirim, an owner of a website that was hosted on sites.google.com brought the case to the European Court of Human Rights (ECrHR) requesting the court to review the justifiability of blocking his website. In this case the Denizli Criminal court blocked access to a website that insulted the memory of Ataturk, a former Turkish president and referred to as the "father of the Turks", but due to technical reasons the entire platform, sites.google.com which hosted other websites was blocked.[49] The ECrHR held that blocking access to an entire platform rather than the offending website breached the right to freedom of expression under article 10 of the ECHR.[50] The ECrHR also stated that the right to freedom of expression applies to the right to Internet access which includes unrestricted access.[51] It stated that article 10 of the ECHR applies not only to the content of information but also to dissemination.

6. Conclusion

Most cyber communication is lawful, but the discussion illustrates that illegal communication poses a serious challenge to law enforcement. An intermediary which may be considered as a gatekeeper to access to and/or exchange of information on the Internet is increasingly under pressure to detect and/or prevent access to unlawful communication. It is important to establish which information-gathering method an intermediary must employ to establish whether communication is unlawful and the circumstances in which an intermediary must block access to and/or remove illegal communication.

Governments must ensure an intermediary is protected against liability where it exercises its discretion to remove or block access to cyber communication. Likewise, the user should have some form of recourse in instances where free speech and/or privacy by means of cyber communication is limited.

The discussion highlights that governments should not shy away from critiquing the manner in which they regulate cyber communication. Countries have different approaches pertaining to Internet governance which reflect their cultural, economic and social circumstances but the right to free speech and privacy inherent to free speech should be

[49] Laidlaw [2] 4 – 5, 21 – 22, 120, 144 – 145.
[50] Horten [37].
[51] Laidlaw [n 2] 199.

protected on national and global level and should only be limited if necessary and proportionate.

References

[1] ABKAR, J. "Thailand to prosecute anyone that even looks at material considered insulting to the monarchy", 2017. Access from: www.dailymail.co.uk/.../Thailand-prosecute-internet-insult-monarchy-king-crop-top.ht.

[2] AHMET, S.Y., SPECKHARD A. "Telegram: the mighty application that ISIS loves," 2016. Access from: http://www.icsve.org.

[3] BILCHITZ, D. "Privacy, surveillance and the duties of corporations" 2016 *South African Law Journal*, 45 – 67.

[4] CHAMBERS-JONES, C. *Virtual Economics and financial crimes* US: Edward Elgar Publishing Limited, 2012. ISBN: 2012935286.

[5] COLEMAN, C. "Robin Hood Airport tweet bomb joke man wins case," 2012. Access from: http://www.bbc.com/network/news/uk-england-19009344.

[6] DAVIS, R. "Pandora's Box: South Africa and the (mis)use of social media", 2017. Access form: https://www.dailymaverick.co.za/article/2017-04-05-pandoras-box-south-afica-and-the-misuse-of-social-media/WT_US60w00o

[7] GIBBS, S. "Facebook under pressure after man livestreams killing of his daughter," 2017. Access from: https://www.theguardian.com/technology/2017/apr/25/facebook-thailand-man-livestreams-killing-daughter

[8] HARVEY, H. *Collisions in the digital paradigm*. Oxford: Hart Publishing, 2017. ISBN 9781509906529

[9] HORTEN, M. "The looming cloud of uncertainty for Internet intermediaries" 2016. Access from: http://www.cdt.org.

[11] LAIDLAW, E.B. *Regulating Speech in Cyberspace*. United Kingdom: Cambridge University Press, 2015. ISBN 978-1-107-04913-0.

[12] LEDERMAN, E. *Infocrime*. United Kingdom: Edward Elgar Publishing Limited, 2016. ISBN 978 1 78536 125 8.

[13] LOWEN, M. "Turkish authorities block Wikipedia without giving a reason", 2017. Access from: http://www.bbc.com//news/world-europe-39754909.

[14] PHIPPEN, J.W. "Why Turkey blocked Access to Wikipedia, 2017. Access from: http://www.theatlantic.com/news/archive/2017/04/turkey-blocks-wikipedia/524859 .

[15] PILLAY, D. “SA looks to criminalise revenge porn”, 2016. Access from: http://www.timeslive.co.za/scitech/201608/30/SA-looks-to-criminalise-revenge-porn

[16] STAUFFER, P. “The Internet is not the enemy,” 2017. Access from: https://www.hrw.org/world-report/2017/country-chapters/the-internet-is-not-the-enemy

[17] TAPSFIELD, J. “This terrorism sent a WhatsApp message and it can’t be accessed,” 2017. Access from: http://www.dailymail.co.uk/news/article-4350264/Rudd-demands-access-encrypted-WhatsApp-messages.html.

[18] VELOCCI, C. “Internet Access is now a basic human right”, 2016. Access from: http://gizmodo.com/internet-access-is-now-a-basic-human-right-1783081865

[19] WATNEY, M.M. “Law Enforcement Access to Password Protected and/or Encrypted Mobile Data” presented at the 11th International Conference on Availability, Reliability and Security, Salzburg, Austria, 2016.