REVIEW OF LEGISLATIONS ON ONLINE CONTENT REGULATION IN THE WORLD

RISHABH PAHWA
IMEITY/2018/03505

TABLE OF CONTENTS

1. Introduction

Vast number of people from children to adult across the world now have access to internet in some form. Over 3.6 Billion people as of 2017 which is roughly half the world population have access to internet. They can access internet on various platforms such as computers, mobiles, laptops and many other devices, as technology is becoming cheaper and readily available. People are starting to become a part of the social networks that exist online to interact with other people, this is not only convenient but also interactive and keeps the user engaged. There are various social networks emerging which include but not limited to Facebook, Twitter, Instagram, LinkedIn etc. Facebook alone has over 2.2B users worldwide as of Q2 2018 and the number is only growing. These platforms are open to all types of users and in many cases can be easily abused by users to spread content like hate speech or other unlawful content. Children can also be exposed to content which is unsuitable for them. This abuse calls for regulations on this online content. Further we will see how these some of these regulations are enforced in various countries across the World.

2. Regulations in Other Countries

2.1 Tanzania

The Electronic and Postal Communications Regulations in Tanzania aims to regulate online content to curb “hate speech” and “fake news”. It gives the authority power to keep a register of bloggers, online forums, online radio and online television, and take action against those who don’t comply with these regulations.

The content which is prohibited from these platforms:

- Hate speech, obscene and indecent content
- Pornography
- Sexual Offenses
- Violent Content
- Torture, killings etc.
- Annoyance, threat of harm, public disorder
- Hate propaganda, hatred etc.
- National security, public health and safety
- Bad language
- False content

A major drawback which comes with this, bloggers, owners of forums and radio and television streaming services are made to register with communications regulator and have to pay a licencing and annual fee. The fee can be as high as 1.1 Million Tanzanian Shilling (Roughly 33,100 Indian Rupees) for a country where 70% of the population lives on less than 130 Indian rupees per day. This has forced many content creators to go offline as they are unable to pay the absurd licensing fee.

The installation of surveillance cameras in Internet Cafe's cannot be justified by reference to the protection public safety or any other legitimate aim. While it may be legitimate for businesses to install surveillance cameras in their premises to prevent shoplifting, this decision should be left to them, not imposed by the State.

Vagueness of terms like "online content providers" leads to a lot of confusion as well. Large online forums have also been shut down since these regulations came into place. Monitoring a large amount of daily comments and deleting any content found inappropriate by the law within 12 hours is a difficult process to be executed. It is also not acceptable for these forums to share user identities with the authorities as many of the users chose to remain anonymous.

However the regulations do have many positive aspects as well. It makes mandatory for users to keep a password on their devices to avoid any misuse of their social network accounts.

The regulations also provide important safeguards for child protection online, which prohibits children's to access to prohibited content online.

In a boost to privacy and data protection, it prohibits unauthorized disclosure of any information received or obtained, except where the information is required for law enforcement purposes. Furthermore, it restricts use of information only to the extent that is necessary for the proper performance of official duties.

Handling complaints is straight forward, if a person feels aggrieved by any matter related to prohibited online content, they may file complaints to the online content provider. On receipt of such complaint, the online content provider must check the content being complained of and remove it within 12 hours.

2.2 Germany

The Network Enforcement Act is applicable to Facebook, Twitter and other social networks commonly referred to as "Facebook Law".

The goal of Network Enforcement Act is the removal of illegal content as per the criminal code which includes:

- Defamation of religions, religious and ideological associations in a manner that is capable of disturbing the public peace.
- Criminal defamation and insult, including insult against a group.
- Publicly approving of, denying or downplaying international crimes committed under the rule of National Socialism, or approving of, glorifying or justifying National Socialist rule of arbitrary force.
- Other content restrictions include prohibitions on: disseminating propaganda or using symbols of unconstitutional organizations, “treasonous forgery” and “dissemination of depictions of violence”

However, numerous legal experts believe that the new law violates the German constitution, particularly Article 5, which guarantees the freedom of expression and the right to information.

The functioning of the Act is designed to be simple for end users of social media, the user can lodge a complaint on the social media platform and a representative within the support team will immediately take note of the complaint and check whether the content reported is unlawful and subject to removal. If the content is found unlawful it is removed within 24 hours of receiving the complaint and the access to other unlawful content is blocked within 7 days. The user will also be notified about the action. The content after removal is stored as evidence for a period of 10 days, which is very beneficial to avoid any conflict in the future.

Social Networks not complying with the Network Enforcement Act and which fill to remove illegal content within 24 hours since the complaint will face hefty fines of up to 5 million Euros. Germany has one of the strongest policies in the world against hate speech and the hefty fine does put pressure on the social networks to take actions more efficiently. Major networks like Facebook have stated that they have hired over 1200 German speaking moderators to review flagged content on their network, and carry out an average of 15,000 deletions every month, there certainly is some progress.

2.3 Russia

Lawmakers in Russia have drafted a legislation that would impose regulations on several social networks. Some of its major features are listed below.

- Every major social network would be required to establish representation in Russia, to make it easier for the Russian authorities to communicate with these companies.
- All major social networks would be forced to identify their users by their phone numbers. This would effectively make it impossible for Russians to use social media anonymously, because individuals have to surrender their passport information when purchasing SIM cards.

- At their own users' requests, all major social networks would be required to delete any information that violates Russian laws. Within 24 hours.
- At the request of Russia's federal censor, all major social networks would have to delete any "unverified publicly significant information presented as reliable information." In other words, the Russian government could force social networks to remove anything it says is "fake news."
- All major social networks would be required to prevent users from publishing content that promotes "pornography or a cult of violence." They would also be required to delete all obscene language.

The process for removing any content from social networks is a simple one, a user can lodge a complaint to the social network support administrator, they have 24 hours to review the complaint and delete it if found illegal. A record is kept of all these complaints for reference.

However, the legislation vaguely specifies what is considered to be illegal and it's kept open to interpretation; this might lead to social networks deleting anything complained for to avoid any complications.

Furthermore, the legislation has procedures for handling "fake news", a state agency if notices any false claim on social media will order the social network to delete the false information within 24 hours. And if failed, the social network will be blocked from Russian internet, as blocking individual pages is not possible.

2.4 Singapore

Singapore, which has a reputation for censorship, has made headlines for its recent attempt to regulate the Internet. Like most countries, Singapore had to amend its laws to capture the Internet. This online censorship is regulated by Media Development authority (MDA).

Singapore has adopted a multipronged approach to Internet censorship. First, the Singapore Broadcasting Authority, which regulates Internet content, has said that the regulations are targeted only at the function of the Internet that is of a broadcast nature. Second, it has adopted the peculiar, perhaps even unique, idea of the class license: certain classes of content are deemed to be automatically licensed provided a code of practice is abided by. In effect, censorship is after, not before, publication. Matters of race, religion and politics are given special attention on the Internet. When the code is breached, the license is revoked [14].

Although the regulators carry the name "broadcasting," the mechanism employed resembles those that apply to the print media. Singapore's regulations are, in the main, an attempt to rationalize regulation of the Internet with regulation of the print media.

In keeping with the reliance on technology, Singapore IAPs have to use proxy servers that have a refused-access list to block access to blacklisted sites--currently a little more than 100, mostly pornographic sites.

2.5 Europe

Europe has adopted the General Data Protection Regulations (GDPR) which is a data privacy measure that regulates the organizations that use peoples' private information such as social network checks how they collect and use the data they collect of the users. It aims to give the users control over their own data.

The new regulation applies a broad definition to what qualifies as personal data. Certainly your name, age, profession, and all the other basic details one would normally list on their social media profiles. But it also covers IP addresses, location data, and web browsing cookies.

Under the GDPR, all organization that concern with user data need to explain what data they are collecting and the reason for collecting the same. And some types of data need user consent for being collected. GDPR asks for high level of transparency from these organizations. This offers much more privacy to the user and security on their personal information.

GDPR will also increase the trust in the organizations which concern with user data, as the users know what data is being collected and how it is being used. It will increase the engagement of the user and improve the overall experience.

Noncompliance to the GDPR implies hefty fines. For the most serious such as exploiting user data without consent, the fine is up to 4 percent of company's annual income, or 20 Million Euros.

Fundamentally, the GDPR is driven by the common sense belief that end-users should be given a clear understanding of exactly what data is being collected when they sign up for a social network, and how the data will be used in future. User data is a valuable asset and these regulations aim to make that value clearer to the end user.

3. Information Technology Act, India

It is an existing act which is closely related to regulating online content in India. The IT Act prohibits a wide range of offenses, these illegitimate actions can be carried out where either the computer is the tool or target or both.

The offences included in the I.T. Act 2000 are as follows –

- Tampering with the computer source documents.

- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Sections which fall in context of regulating online content are:

1) Section 66B includes punishment for dishonestly receiving stolen computer resource or communication device.
2) Section 66C includes punishment for identity theft
3) Section 66D includes punishment for assuming identity of another person with intent to deceive.
4) Section 66E includes punishment for violation of privacy
5) Section 67 prohibits publishing or transmitting obscene material in electronic form. This includes:
    - Material containing sexually explicit act, etc.
    - Material depicting children in sexually explicit act, etc.
    - Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information
6) Section 73 prohibits publishing Electronic Signature Certificate false in certain particulars.
7) Section 74 prohibits publication for fraudulent purposes. This includes, knowingly creating, publishing or otherwise making available an Electronic Signature Certificate for any fraudulent or unlawful purpose.

3.1 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011

We cannot imagine our lives without computers, laptops, mobiles, internet and other gadgets which facilitate us to acquire/share knowledge and help us to be effective communicators. This the positive side of the technology. There is also negative side of technology which is becoming a source for committing cyber-crimes such as hacking of computers, stealing of pass words, confidential data, etc. Although Information Technology Act,2000 provides for certain safeguards for data protection and to prevent misuse of data etc., there are still some grey areas which always necessitate changes in the Act or framing of new rules. The focus of this article is on the new rules called "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 and their implication.

This applies to all bodies corporate which handle sensitive personal information or data in a computer resource. This section provides that if a body corporate is negligent in implementing and maintaining reasonable security practices and procedures and causes loss or gain to any other person, it shall be liable to pay damages to the person affected. It further says that sensitive personal information or data shall be prescribed by the Central Government in consultation with professional bodies or association. However till recently the same has not been notified by the central government. The leakage of credit card number by an Indian BPO Firm prompted the Government to frame and publish the Rules in order to prevent such happenings in future.

The most important aspect of the new rules is that Sensitive personal data or information has been defined by Rule 3. Sensitive personal data or information of a person means such personal information which consists of information relating to:

- Password
- Financial information such as bank account or credit card
- physical, physiological and mental health condition
- medical records and history
- Biometric information
- any detail relating to the above clauses as provided to body corporate for providing service

- any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise

However information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Privacy Policy to be published on Website:

Everybody corporate or any person who on behalf of the body corporate collects, receives, possess, stores, deals or handles data shall provide a privacy policy for handling of or dealing in sensitive personal information. And such policy should be published on web site of the body corporate and must be available for view by provider of information.

The web privacy policy must disclose the following:

- Type of personal or sensitive information collected
- Objective of collection of personal sensitive information and type of information collected and its purpose and usage
- Method used and manner of storing data collected
- Safety procedures, system checks followed for storing and protection of data
- Method and manner of Disclosure of sensitive personal information to any third party is made
- Grievance redressal procedure

Method and manner of Collection of information:

Rule 5 lays conditions for collection of information:

- It requires body corporate or any person on its behalf to obtain consent of the provider of information through fax or e-mail before collection of information.
- Option should be given to the person to give or not give personal sensitive information and also option to withdraw his consent.
- Personal sensitive information shall not be collected unless such collection is necessary for a lawful purpose
- It shall be used only for the purpose for which it is collected.
- Body corporate shall appoint a grievance officer

Prohibition on Disclosure of Information to 3rd parties:

The new rules provide that disclosure of any sensitive personal information to any third party shall require prior permission of the provider of information. However an exception has been made to provide the information in case the government agency requires it for the purpose of investigation of any cyber-crimes. But the Government in such cases shall state that it shall not publish or share it with any other person.

Prohibition on Sharing of Information:

There is a prohibition of transfer of sensitive personal information and other data to any other body corporate or a person in India or abroad. Transfer or sharing with other body corporate is permitted provided the other body corporate in the following cases:-

- the receiver has the same level of data protection as that of body corporate and
- Transfer of data is necessary for performance of the lawful contract.

3.2 Information Technology (Intermediaries' Guidelines) Rules, 2011

The Information Technology Amendment Act, 2000 has clarified the definition “Intermediary” by specifically including the telecom services providers, network providers, internet service providers, web-hosting service providers in the definition of intermediaries thereby removing any doubts. Furthermore, search engines, online payment sites, online-auction sites, online market places and cyber cafés are also included in the definition of the intermediary.

Under Rule 1 the intermediaries are obliged to publish the rules and regulations, privacy policy and user agreement for access to intermediary’s computer resource.

Under rule 2 the rules and regulations are defined, the user is prohibited to host, display, upload, transmit, update or modify information that:

1. belongs to another person and to which the user does not have any right to
2. is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever
3. harm minors in any way
4. infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force

5. deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature
6. impersonate another person
7. contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource
8. threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation

Intermediaries cannot knowingly host or publish the content mentioned in rule 2, they have to remove content prohibited under these Rules. To save itself from being liable to compensation the Intermediaries would have to determine whether the content violates the several terms which are ambiguous in nature. There are also several other rules which the intermediaries have to abide by, these are very effective in regulating intermediaries.

4. Other Indian legislations

4.1 Cigarettes and Other Tobacco Products Act

Prohibition of advertisement, promotion and sponsorship of all tobacco products.

Section 5 of Tobacco Control Act provides:

- Both direct and indirect and indirect advertisement of tobacco products prohibited in all forms of audio, visual and print media.
- Total ban on sponsoring of any sport and cultural events by cigarette and other tobacco product companies.
- No trade mark or brand name of cigarettes or any tobacco product to be promoted in exchange for sponsorship, gift, prize or scholarship.
- No person, under contract or otherwise, to promote or agree to promote any tobacco product.

Amendment rules notified in 2005

- Ban on sale of tobacco products through vending machines
- Ban on sale of tobacco products by minors
- Restrictions on the content, size and number of point of sale of advertisements.
- Ban on visible stacking of tobacco products at point of sale to prevent easy access to minors.

- To prevent brand sharing and surrogate advertising of tobacco product; 'indirect advertising' has been comprehensively defined.
- Ban on display of tobacco products or their use in movies or television
- Health warning to be placed as a prominent bottom scroll in cinema and television programs, which have been produced prior to this notification.
- Ban on display of names/logos of tobacco brands in any manner during media coverage of international events sponsored by tobacco manufacturers.

4.2 Press Council Act, 1978

The Press council of India is a statutory body in India that governs the conduct of print and broadcast media. It has supreme power in regards to the media to ensure that freedom of speech is maintained. The Press council act is to establish a council for the purpose of preserving the freedom of the press and maintaining and improving the standards of newspaper and news agencies. The council is also responsible for building up a code of conduct for newspapers, news agencies and journalists in accordance with high professional standards.

4.3 Cable Television Networks (Regulation) Act, 1995

Prior to the enactment of the Cable Television Networks

(Regulation) Act, 1995, the cable industry had been completely unorganized and unregulated. The Act was intended at curbing a perceived 'cultural invasion' by regulating the content of the programmes being telecasted and by providing some accountability from cable operators. The Act provides for the mandatory registration63 for all cable operators. Along with other mechanisms it also defines the Programme code and Advertisement Code to regulate the programmes and advertisements transmitted by cable operators.

The Programme Code prohibited several things from being transmitted, some of these include which:

- Offensive content
- Criticism against friendly countries
- Attack against religions
- Obscene and defamatory content
- Encourages violence
- Denigrates women or children
- Encourages superstition or blind belief
- Affects the integrity of the Nation

Also, the Advertising Code prohibits content which:

- Derides any race, caste, colour, creed and nationality
- Encourages violence or crime or glorifies violence or obscenity in any way

- Exploits social evil such as dowry, child marriage
- Promotes directly or indirectly, sale of cigarettes, tobacco, wine, alcohol, liquor or other intoxicants.
- Is against any provision of the Constitution of India
- Presents criminality as desirable

4.4 Press and Registration of Books Act, 1867

The objective of this act is to secure the information relating to the printing establishment and their publications, to regulate printing press and newspapers, to preserve and register copies of every book and newspaper printed in India and to prevent publication of anonymous literature.
Every owner of the Press (for printing books, newspapers, periodicals and papers etc) must make a declaration before the district/metropolitan/Sub divisional magistrate of that area.
Printer and Publisher of every newspaper subscribe a declaration before the concerned District/Metropolitan/Sub divisional Magistrate
Every book, paper or newspaper shall print the name of the editor, printer publisher, address of printing place and place of publication. If the language, ownership or place of printing or publishing is changed, a new declaration shall be necessary.
Every printer shall deliver copies of the book, newspaper or periodical with a memorandum containing the title page, language, periodicity and all related information to the public library, free at his cost.

4.5 The Cinematography Act, 1952

Censor Board, is a Government's regulatory body. It is controlled by Ministry of Information and Broadcasting. It reviews, rates and censors movies, television shows, television advertisement and promotional material. It regulates the public exhibition of films in India under the provisions of 175 the Cinematograph Act, 1952. Films can be publicly exhibited in India only after the certification by the board. The CBFC currently issues the following certificates:

1. Universal (U): All ages admitted, there is nothing unsuitable for children. Films under this category should not upset children over 4 year.
2. Parental Guidance (U/A): All ages admitted, but certain scenes may be unsuitable for children under 12 years.
3. Adult Only (A) : Only adults are admitted, no body younger than 18 can rent or buy an 18 rated VHS, DVD, Blu-ray Disc, UMD or game, or watch a film in the cinema with this rating. Films under this category do not have limitation on the bad language that is used. Hard drugs are generally allowed, and strong violence or sex references along with non-detailed sex activity is allowed.
4. Restricted to any special class of persons: This rating signifies that the film is meant for a specialized audience, such as doctors.

4.6 The Indian Copyright Act, 1957

Copyright is a right given by the law to creators of literary, dramatic, musical and artistic works and producers of cinematographic films and sound recordings. It includes rights of reproduction, communication to the public, adaptation and translation of the work. Generally this copyright lasts for 60 years and protects the rights of creator.

The Copyright Act prohibits making infringement copies for sale or hire or selling or letting them to hire. It prohibits trading and distribution of these copies. This may as well occur in an online transmission such as in form of electronic mail and the rights of the author/creator must be protected in such case.

5. Context

There are many common features in all models but they all have their differences. Every country has its own approach to regulate online content. A major implication from studying the various models in different countries is that there will not be one universal model for regulating the Internet. But this does not mean that the regulatory wheel must be reinvented each time. The various countries presented in this paper provide enough models to follow.

An approach to Internet content regulation based on the cultures of each country makes the most sense. This is what it means to be an international community, rather than a commune, or even a barracks. It would require that the world learns to step back, check the lenses that they use, and try to accommodate the differences. Perhaps the free-flowing and anarchistic Internet culture will gradually evolve to include these pockets of differences.

6. Recommendations

As other countries, Internet in India is getting more and more accessible to the people across all ages, and they are increasingly getting connected on social network websites, which come with both their advantages and disadvantages. These platforms are open to everyone and they can be easily manipulated to spread hate speech and other unlawful content as already seen earlier. This public also includes a vast number of children which can be exposed to content which is not suitable for them. Due to these things there has been an increasing importance for self-regulating mechanism for Online Content, especially in India with over 460 million internet users making India the second largest online market, and with the highest number of Facebook users in the world at a staggering 270 million user, and these numbers are only increasing every day. As it is already observed in case of Television content, self-regulation works very well and the same needs to be done for online content.

Intermediaries must be set up self-regulating mechanism to take control of the situation in India, the authorities will form a code of conduct for online platforms to abide, and anything which is found to be against this code will have to be removed in the stipulated time period such as 24 hours after a complaint is lodged. The authorities can also determine what is considered to be "fake news" and be able to notify the online platforms to remove such content within a stipulated time period say 24 hours.

Prohibitions should include the existing ones which are applicable to content if transmission is happened through internet/mobile communications infrastructure, which are discussed previously. These prohibitions should include, but not limited to:

- Hate speech, obscene content.
- Defamation of religions and ideology in any manner that may disturb public peace.
- Criminal defamation and insult, including insult against a group.
- Pornographic content, esp. involving children.
- Hate Propaganda, hatred etc.
- Fake news, which would be determined by the authorities.
- Violent content.
- Torture or killing.
- National security, public health and safety.
- Annoyance, threat of harm, public disorder.

Additionally, the intermediaries may make it mandatory for users to enter their phone number or some sort of identification when creating a social network account, this will curb the issue of fake profiles and accounts which are often used to spread unlawful content as mentioned above.

At the request Indian authorities, all major social networks would have to delete any fake/false news and block all access to it within 24 hours.

To establish regulation of online content, the provider of the social network should include representatives within the support team which take note of any complaints regarding any wrong content which is not suitable. The end user should be able to easily lodge a complaint on the platform itself and get a timely response. This team of specialized representatives should be able to understand the native languages as well, for better understanding. There should be a fixed time such as 24 hours within which the content must be checked and removed if it doesn't meet the community standards, and in case of removal the content must be stored for purpose of evidence.

In case the provider of social network fails to respond to the complaint in given time, the user should be able to contact the authorities with an easily accessible online form. The authorities

can then verify the complaint and if the reported content is found to be unlawful, they can notify the social network provider to remove it within a stipulated time period such as 7 days, penalty may be levied in case they fail to do so. This will provide an effective mechanism to control the online content, providing the user an additional option in case their complaints are not responded in due time.

7. References

1. https://www.statista.com/
2. https://www.article19.org/wp-content/uploads/2018/05/Tanzania-Online-Content-Regulations-2018-Final.pdf
3. https://www.theverge.com/2018/7/6/17536686/tanzania-internet-laws-censorship-uganda-social-media-tax
4. https://www.voanews.com/a/tanzania-moves-to-regulate-online-content/4362731.html
5. https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf
6. https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight
7. https://www.lexology.com/library/detail.aspx?g=b1dd56e4-adbf-4811-9b74-e8ebcd4f4217
8. https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law
9. http://www.legalservicesindia.com/law/article/982/6/Reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information
10. https://cis-india.org/internet-governance/constitutional-analysis-of-intermediaries-guidelines-rules
11. http://shodhganga.inflibnet.ac.in/bitstream/10603/36776/12/12_chepter%203.pdf
12. https://www.isoc.org/inet97/proceedings/B1/B1_3.HTM
13. http://www.singaporelawreview.com/juris-illuminae-entries/2015/internet-regulationa-myth-in-singapore
14. https://www.lexology.com/library/detail.aspx?g=c7f9083d-635c-484a-9b5b-ff3b077d4e22
15. https://www.article19.org/resources/russia-increased-internet-regulation-poses-serious-challenge-to-online-expression/