DID THE INDIAN GOVERNMENT DO RIGHT BY BANNING THE CHINESE APPS

Written by ***Jayalakshmi Venkatraman***

3rd Year BCOM LLB Student, SASTRA Deemed University, Thanjavur, Tamilnadu, India

ABSTRACT

"A nation's ability to fight a modern war is as good as its technological ability" ~ Frank Whittle. One of the most crucial decisions taken by the Government of India was the banning of the Chinese apps which were considered to be a threat according to Section 69A of the Information Technology Act, 2000. These apps have been banned ever since as they were considered to be "engaged in activities which are prejudicial to sovereignty and integrity of India, defense of India, security of state and public order." This Research Paper co-authored will first give a brief about why we brought the cyber laws into this topic and how we related this with the banning of apps from China. The main stress in this paper was given to the legality and the effects of banning by the various laws that are applicable in the Indian region along with the relevant cases that can be mentioned. The paper also gives an overview about the emergency banning and the process that has to be followed according to the Information Technology Act. We have tried to give a broader understanding about the various other laws other than Section 69A such as Article 19(1), Article 19(2) and Article 14 of the constitution that can be applied. This research is done with the already existing research material to include the various judgements and the various laws that can be given as a possible explanation for this topic in specific.

Keywords: Chinese apps ban, Information Technology Act, 2000, Data Security, Privacy

INTRODUCTION

Cybercrime is a relatively new type of crime in the world. Any illegal behavior that occurs on or through the assistance of computers, the Internet or other technology recognized by the "Information Technology Law" is considered a cybercrime. Cybercrime is the most common crime in modern India and its impact is devastating. Criminals not only cause great harm to society and the government, but they also hide their identities to a large extent. A variety of illegal acts are carried out by highly skilled criminals on the Internet. In a broader sense, cybercrime can be defined as any unlawful act in which a computer or the Internet is used as a tool, a target, or both. The term "cybercrime" has been interpreted by Indian courts on a number of occasions, although it is not defined in any statute or statute passed by the Indian legislature. Cybercrime is an uncontrollable crime that stems from the abuse of modern society's growing reliance on technology. The use of computers and other related technologies in daily life is increasing rapidly and becoming the need to support the convenience of users. It is an unlimited and non-quantifiable medium. Cyber harassment, cyber terrorism, email spoofing, email bombing, cyber pornography, cyber defamation and other emerging cybercrimes are just some of the emerging cybercrimes. If committed using a computer or the Internet, some traditional crimes may fall under the category of cybercrime.

On June 29, the Indian government banned apps from China (companies based in China). This change belongs to the IT department, which is appealing for its power to ban apps under Section 69A of the IT Act. The ministry said a mobile app was used to steal user files. It also said there was an illegal transfer of data to servers outside India. Banned apps include apps related to e-commerce, games, social media, Glance, instant messages, and file sharing. These include widely used Chinese apps such as TikTok, Share-it, WeChat, Club Factory and Cam Scanner.

TYPES OF CYBER CRIMES

Email spoofing:

This technique is email header spoofing. This means that the message appears to have been received from someone or somewhere that is not an authentic or real source. These tactics are

often used in spam or phishing campaigns because people are more likely to open an email or email when they believe the email was sent by a legitimate source.

Spam:

Spam emails, also known as spam emails. This is an unsolicited mass message sent via email. The use of spam became widespread in the mid-1990s, and that is the problem most email users face today. The recipient's email address is collected by a spam program, which automatically scans the Internet for email addresses. Spammers use spam bots to create email distribution lists.

Online defamation:

Online defamation is behavior that damages an individual's reputation in the eyes of another person through cyberspace. The purpose of making a defamatory statement is to damage an individual's reputation.

IRC Crime (Internet Relay Chat):

IRC servers allow people from all over the world to come together under a platform sometimes called a room, and they chat with each other.

Phishing:

In this type of crime or fraud, attackers try to obtain information such as login credentials or account information by impersonating a reputable person or organization in other communication channels. each other or by email.

Software piracy:

It may be described as the copying of software programs unauthorizedly.

Copyright infringement:

It may be defined because of the infringements of a person or business enterprise's copyright. In easy time period it is able to additionally be described because the use of copyright substances unauthorizedly which includes music, software program, textual content etc.

DOS assault:

In this assault, the attacker floods the servers, structures or networks with site visitors in an effort to crush the sufferer sources and make it infeasible or tough for the customers to apply them.

Email bombing:

It is a form of Net Abuse, in which massive numbers of emails are dispatched to an email deal with in an effort to overflow or flood the mailbox with mails or to flood the server in which the email deal with is.

Salami assault:

The different call of Salami assault is Salami slicing. In this assault, the attackers use a web database in an effort to capture the customer's facts like financial institution information, credit score card information etc. Attacker deduces little or no quantities from each account over a length of time. In this assault, no grievance is recorded and the hackers continue to be loose from detection because the customers continue to be ignorant of the slicing.

IMPACT OF THE BAN IN CHINA

The Chinese government blamed this Indian government's method of banning Chinese apps in India, calling it discriminatory and a violation of WTO rules. Before we dive into such claims, it is important to note that China has also banned major websites like Facebook, YouTube, Twitter, etc. for reasons of national security and sovereignty. One of the most affected Chinese companies instead of this ban is "Byte Dance ltd.", a Chinese multinational company based in

Beijing and developer of several apps banned in India. The Indian market is of prime importance for the company as the revenue from this market is huge. During a month-long temporary restraining order earlier, the company told a local court it was losing $15 million a month, as reported by Reuters. Overall, it can be said that Chinese companies have certainly been hit the hardest of all the parties involved.

IMPACT OF THE BAN IN INDIA

Out of the 10 most downloaded apps in India, 6 of them are Chinese, if you put it in the numbers, it's a completely different ball game, with over 100 million numbers. There's no denying that some users have been hit hard by the banning of these apps as they infiltrate people's daily lives. Apps like CamScan that people use every day to save important documents, game apps like PUBG have become extremely addictive for some and also considered a concern by some. Indeed, TikTok allows users to share their thoughts and creativity and provides a platform for people to move forward, especially during lockdown, all serving a large portion of the population of India. Although if one looks at it from a positive perspective, this will now enable the growth of applications and pave the way for India to become an IT superpower, competing with USA, UK, Australia, etc. and create a strong foothold in this field. It is not about participating in the global IT market; it's about taking on leadership positions.

India also sends a strong message to the world in general and China in particular that it is not dependent on or a victim of Chinese policies. Though it is equally important to realize that this move could harm India in the sense that it could take away a lot of investment that could have been received from Chinese IT companies. On the day the app was banned on TikTok, its Indian counterpart called “Chingari” saw its downloads increase from around 1 Lakh to over 1 Crore.

LEGALITY OF THE BAN ACCORDING TO INDIAN LAWS

Scope of Section 69A of the Information Technology Act:

Section 69A of the Information Technology Act 2000 was introduced in a 2008 amendment to the Act. This gives the central government the power to block public access to any information online, whether it's a website or a mobile app. If a website threatens India's defense, sovereignty and integrity, friendly relations with other countries, or public order, the government may follow its due process and ban it under Section 69A. Detailed procedures for doing this are set out in the Information Technology (Procedures and Safeguards for Blocking Access to Information by the Public) Regulations, 2009. Alternatively, courts can order blocking of information on the internet. Telecommunications authorities can also issue blocking orders to internet providers to enforce license terms.

Section 69A requires that each central government agency, state, and federal territory have a focal point, to receive complaints about websites hosting "offensive" content. Once the lead officer realizes the value of the complaint, he passes it on to a designated officer, who chairs a committee to review the complaint. The committee consisted of representatives from the Departments of Law and Justice, Home Affairs, Information and Broadcasting and India's Computer Emergency Response Team (CERT-In) and heard the middleman. Once this procedure is complete, the Designated Officer may issue instructions to block a website, only with the approval of the Minister of Information Technology - under normal circumstances.

Section 69A also makes room for an "emergency" event, in which the Designated Officer reviews the request for containment, and makes recommendations to the Secretary of the Department of Electronics and Information Technology, which on the basis of temporary office, can give instructions. to block a website. In such cases, the aggrieved party is not entitled to a hearing.

However, within 48 hours after the temporary orders are approved, the designated official must bring the blocking request before the committee. The designated official will then issue a notice on the website asking his representative to appear before the committee at a specific date and time. The site has at least 48 hours to prepare for the hearing. The committee's proposal is forwarded to the IT secretary, who has the final say and can approve the request. The Clerk

reserves the right to refuse a block request and give instructions for unblocking the site. Section 69A also provides for a review committee, which meets every two months to review guidelines issued to block a website. It can cancel a block order if legal procedures have not been followed. The latest order banning 59 Chinese apps is a temporary order, issued under emergency provisions. The application companies were given the opportunity to appear and submit their explanations before the committee.

One feature of Section 69A is that it includes terms such as "national security, urgency, sovereignty and integrity of India and public order", which are common to decisions about security. national security in Indian law. The section requires strict confidentiality regarding claims and actions taken. Due to the presence of this provision, Right to Know (RTI) requirements are not applicable under the law. In addition, the application and appeal examination committees are entirely composed of members of the executive board. In its 2015 ruling on the landmark case *Shreya Singhal v/s Union of India*[i], the Supreme Court of India upheld Section 69A and existing containment proceedings. The court said the law was constitutional and a website could only be blocked based on a reasonable order. The Supreme Court also pointed out that the law provides adequate protections that an order can only be issued with committee approval to block a website after receiving a response from the aggrieved party. As mentioned in the Rules, in all cases, urgent or not, the reason for website blocking must be documented in writing.

The notice is backed by legislation, i.e., Section 69A of the IT Act, which allows the government to impose geo-blocks targeting specific websites.

Section 69A covers substantive and procedural safeguards against unreasonable (though imperfect) restrictions on Internet access. However, as noted in this Aarogya Setu legitimacy test report, courts are rarely concerned with not having specifically enumerated legal protections to restrict fundamental rights. . As long as the notice itself has sufficient legal force (i.e., it is contemplated under applicable law), it would be hard to argue that the China app ban notice was not contemplated under Section 69A. The strategic interest cited in the announcement sought may also be considered legitimate, particularly in the context of the potential for external aggression.

Relating Article 14, Article 19(1) and Article 19(2) along with the ban issued:

Any account of freedom of expression that does not consider how this ban will affect already marginalized communities is disingenuous at best. Since apps that provide a platform for expression and allow for the dissemination of information are protected by Art.19(1)(a) of the Indian Constitution, a constitutional challenge to the ban is likely.

The Kerala High Court in *Faheema Shirin v. State of Kerala*[ii] recognized that interfering with someone's access to the internet violates inter alia their fundamental right to privacy.

Later, the Supreme Court in *Anuradha Bhasin v. The Union of India*[iii] recognizes that the indefinite shutdown of internet access may constitute an abuse of power. However, he failed to reaffirm the position established by the Supreme Court of Kerala. However, since Faheema Shirin's decision was not subsequently overturned, it is of great persuasive significance and should be properly acknowledged as the correct position in the law. Therefore, assuming that there is a right to freely access the Internet under Article 19, it is important to assess the impact of geo-blocking of Chinese applications on this right. For freedom of speech and expression to be meaningful, the law must be inclusive and accessible to all; It's not just people who have the social capital needed to access apps with relatively complex and hard-to-reach user interfaces. This is especially true given the low level of digital literacy in India. Freedom of expression in this context should be understood to include the manner or background in which people wish to express themselves. Furthermore, while one must assume that the freedom to engage in commerce or business is not reserved for Chinese (perhaps foreign) app developers, they still exercise their right to resist under Article 14.

In *Puttaswamy (Retd.) vs. the Union of India*[iv] as well as in the decision of the Modern College of Dentistry, the Supreme Court reaffirmed that rights cannot be considered as separate compartments. They should be seen as a web of interlinked liberties that complement each other. The most obvious permission related to geo-blocking is the basic permission to access the Internet. Certainly, the basis for imposing such a restriction should be one of the listed conditions mentioned in Article 19(2) (i.e. public order, national security, etc.). However, at the same time, because of the interconnected nature of constitutional freedoms, it must also be fair, just and reasonable under Article 14. This means that geo-blocking cannot be imposed arbitrarily.

This right under Article 14 is open to both citizens and non-citizens. Thus, the Press Information Office announcement is likely to make two separate claims based on equal rights under Article 14. The first, by the Chinese tech giants, who have been concerned about different treatment from applications developed in other jurisdictions with similar capabilities. incompatibility with, among other things, privacy concerns. India under Article 226 of the Constitution.

For geo-blocking to be fair, just and reasonable, it must comply with Article 14 which states that all people are treated equally before the law. However, Article 14 permits different treatment between two different classes provided that the classification between them is reasonable.

In *People's Coalition for Civil Liberties v. Union of India*[v], in a challenge to the constitutionality of Section 5 of the Telegraph Act, 1885 (i.e., the provision allowing wiretapping), SC clarified that the threshold of public emergency was even higher than the grounds specified in Article 19(2), of the Constitution. The Court defines a state of emergency as "the emergence of a sudden situation or condition affecting the entire population that calls for immediate action".

The nature of the concern of public danger should be shown in its color from the restrictions listed in Article 19(2) (e.g., national security). Since the threshold for triggering a public emergency is even higher than the conditions listed in Article 19(2) (conditions discussed below), the decision to skip the pre-sentence hearing before applying geo-blocking may be unwarranted.

Applicability of the Rule 9 of the Blocking Rule Act, 2009:

Rule 9 of the 2009 Blocking Rule empowers the government to impose geo-blocking without creating an opportunity for an online intermediary (i.e. an entity providing online services, e.g. Chinese app) has a chance to listen. Given that TikTok and other intermediaries (e.g., internet service providers) were given a hearing after the decision was made, it seems likely that the basis for geo-blocking is rule 9. This may be the case. which means that the government must assume there is an "urgency" to impose geo-blocking.

CONCLUSION

This is a big step by the government of India to make India an independent country and the promotion of the Voice for Local and Made in India program has begun to turn India into a sub-autonomous country. depends on China for almost everything. This action was taken following an in-depth investigation by the Department. In addition to India, countries such as Australia, Germany, the UK, and even the US have also raised privacy and security concerns with Chinese apps and have adopted strict cybersecurity protocols to guard. This step will help Indian companies and startups gain new customers and increase their user base.

Many Indian companies have started working to create alternatives to banned apps. This will also contribute to the growth of the IT sector in India. The main purpose of banning these apps is to protect the important data of users within the borders of India. RBI has convinced many companies like Paytm, WhatsApp, Google to set up their cloud storage/database in India so that data can only be kept within Indian borders, previously stored outside India in the cloud database. The move will bring more investment in data centers in India. This step is a kind of retaliation by the Indian government against the Chinese government for not properly handling sensitive and important user information and mishandling user data. India needs proper data protection laws, so next time someone will have to think twice before misusing user data. The Personal Data Protection (PDP) Bill 2019 is the first step taken by the Government of India to legislate at the national level on the issue of data protection. Thus, banning Chinese apps has shed light on many issues related to privacy and data security. As responsible citizens of India, we should all stop using these apps and support the government's decision and make India a stronger country both economically and politically.

REFERENCES

1. https://www.jetir.org/papers/JETIR2007375.pdf
2. https://thewire.in/tech/india-ban-chinese-apps-tiktok-legal
3. https://theprint.in/opinion/can-chinese-apps-appeal-india-ban-section-69a-of-it-act-has-answer/455316/
4. https://medium.com/legis-sententia/national-article-writing-competition-2020-rank-10-fffee52a4e16
5. https://www.ijlpa.com/_files/ugd/006c7e_bf23b86e284e4c86922ec23744876227.pdf?index=true
6. https://www.latestlaws.com/articles/critical-analysis-of-legality-of-chinese-apps-ban
7. https://www.legalservicesindia.com/law/article/1841/28/Ban-On-Chinese-Apps-In-India

ENDNOTES

[i] Shreya Singhal v/s Union of India (2013) 12 S.C.C. 73

[ii] Faheema Shirin v. State of Kerala WP(C) No. 19716 of 2019 (L)

[iii] Anuradha Bhasin v. The Union of India W.P {C} No. 1031 of 2019

[iv] Puttaswamy (Retd.) vs. the Union of India (2017) 10 SCC 1, AIR 2017 SC 4161

[v] People's Coalition for Civil Liberties v. Union of India AIR 1997 SC 568, (1997) 1 SCC 301