

RISE OF OTT PLATFORM: A CRITICAL ANALYSIS

Tanvin Anand* & Nidhi Kaushik**

Abstract

The pandemic has restricted all of us to our houses and left us with no option for consuming content be it in entertainment or infotainment sector while sitting at home itself. This has led to increase in the revenue for the OTT platforms and News Portals that operate through digital medium. Since every contents is easily available online these days it becomes extremely important for us to keep in mind the Privacy and the Human Rights issues that are going to be affected. This paper tries to elucidate the recent development in the OTT space and also the laws pertaining to human rights and democracy which are likely to be affected due to the increase in the number of online content shows. It also lays down about how the content can be moderated in the online space meanwhile creating a balance between the rights of the general public and the rights of the creators. Keeping in mind that there are many facets to the human rights law, we will be discussing particularly about the marketized and structural form of human rights which are likely to be hampered due to less or no control over these online platforms. This paper will critically analyse the need of governance over these platforms and how it is likely to be a boon or bane for both the general public and creators. Also, this article will broadly discuss about the procedure used by big online media platforms to evaluate and process personal data for achieving their business model. The aim of this paper is to lay a proper outline for the easy and successful drafting of laws pertaining to the OTT sector. The new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 try to narrow down certain rules and regulation about digital space but those laws are insufficient as far as governance of digital space is concerned.

* Student: B.A.LL.B.(H) @ Amity Law School, Noida

** Assistant Professor @ Amity Law School, Noida

INTRODUCTION

With the advent of the COVID 19 pandemic we all have been confined within the four walls of our houses. The first few months of the pandemic were tough for the entertainment industry as before this everything was being displayed on the big screen but with the advent of the pandemic many restrictions were imposed on the public where we were expected to wear masks and follow social distancing guidelines. The consequences for this restriction aimed from lower attendance at film festivals to getting no viewership thus leading the big production houses to adopt for the OTT platform or else face damages.

RECENT TRENDS IN VIEWERSHIP

Few years back OTT platform was totally a novel concept with limited viewership. Only Netflix used to rule in the online content space but after the pandemic many new OTT platform have come into existence. This is due to the restrictions imposed by the government on the movement of the people and the ease of watching the online content like movie and concerts at just a click of a button. According to a recent study India houses 95 OTT platforms which received an increase of 35% of viewership (Table 1).¹ With the data plans becoming cheap and people having ample amount of time in hand the data hackers also increased.

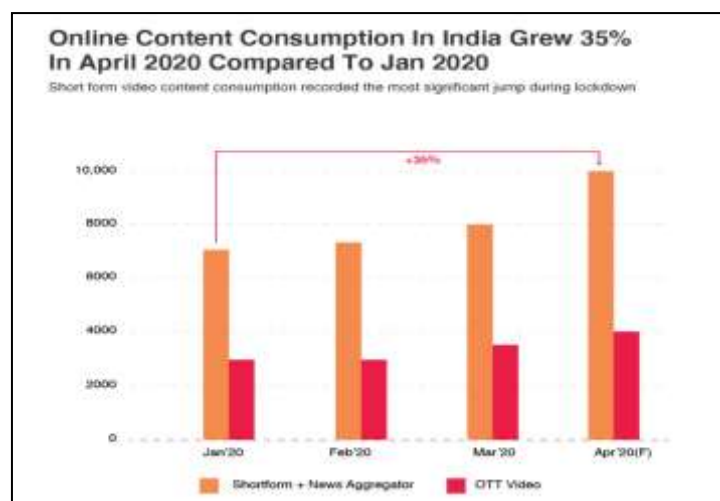


Table 1

A leading OTT platform, Zee5, was caught up in a data breach in which 9 million users data containing names of the users, their phone numbers, associated email addresses and their Zee5

¹ NOW STREAMING: INDIA'S OTT MARKET LANDSCAPE REPORT, 2020 INC42 MEDIA, Available at: <https://inc42.com/buzz/binge-on-datalabs-indias-ott-market-landscape-report-2020/> (Accessed on: Nov 5, 2021)

usernames were leaked online and this is not the first time that something like this has ever happened. Earlier Netflix, Amazon Prime Video, and Disney+, have also been involved in similar data breaches. With an estimated increase of viewership and revenue of \$35 billion² the amount of cyberattacks will also increase and hence a proper mechanism is required to protect the data of the users from getting compromised.

PANDEMIC AND CYBER CRIMES

The cyber-crime cases increased to 50,035 from 44,735 a year before according to a report published by the NCRB. Smaller cities were more vulnerable to cyber threats as majority of the cases were reported from Telangana, Orissa, Assam, Bihar and Jharkhand. The OTT platforms were becoming more prone to phishing attacks which were aimed at collecting the financial information. Also, frauds like malware attacks and ad ware attacks increased during COVID times. In order to the gravity of these crimes we will first give a brief overview of such attacks.

Various Forms of Cyberattacks

- **Phishing Attacks:** A phishing attack means any financial fraud that is carried out online which leads to stealing of credit card/ debit card, password and OTP. It includes a message which at first glance looks to be legitimate by all means. This message is sent over email, website, text or social media.

A very famous case in this regard is that of **NASSCOM v. Ajay Sood**.³ Under this case NASSCOM hired a placement agency (the accused) for carrying out its recruitment process. The Delhi High Court in this regard held that even though phishing is not defined under Indian law it can be described as any online financial fraud wherein the attackers pose to be a legitimate bank and then steal crucial data of the users.

- **Pharming:** Pharming is a portmanteau of the words phishing and farming wherein the website traffic is manipulated and then crucial data of the user is stolen. In order to carry out this kind of crime the attacker will install a malicious code on victim's computer or server which will then trick the user into entering his confidential details on a website.

² OTT SECTOR HAS EXPLODED GLOBALLY AND SO HAS HACKERS' INTEREST IN IT. LEARN HOW TO BEAT HACKERS TO PROTECT YOUR REVENUE APPSEALING, Available at: <https://www.appsealing.com/ott-sector-has-exploded-globally-and-so-has-hackers-interest-in-it-learn-how-to-beat-hackers-to-protect-your-revenue/> (Accessed on: Nov 5, 2021)

³ 119 (2005) DLT 596

In this regard several legislations are already there such as the Information Technology Act, 2000 which does not explicitly give about the definition of Phishing but defines identity theft which indirectly gives an indication about Phishing.

SECTION 66C: Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

SECTION 66D: Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

THE LEGAL ANGLE

Most of the entertainment industry is dependent on a number of agreements which are time bound but since the pandemic was a sudden change in how the usual contracts and agreements are enforced it was a huge problem for the entertainment lawyers to apply the already. Also the pandemic also pushed the entertainment industry to the online space which was at that time not secure.

This brings us to the realisation that Social Media platforms like Twitter, Facebook and Instagram were not the only platforms that were on a rise during the pandemic but also the OTT Platforms like Netflix, Amazon Prime saw a substantial rise during the pandemic.

While there are no rules and regulations explicitly mentioned for the OTT platforms but there are certain sections and articles in other acts which can cover the current need arising in the OTT Sector like Section 67A, 67B and 67C of the Information Technology Act, 2000. These Sections particularly deal with penalising and imprisonment who are found actively engaging in the transmission of sexually explicit and obscene material.

The Ministry of Information and Broadcasting came up with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021) in order to regulate the kind of content being transmitted online. These rules will have an overriding effect over the old Information Technology (Intermediary Guidelines) Rules 2011. The new Act

branches out two categories for entities which are as follows: Social media intermediary and significant social media intermediary.

- **Social Media Intermediary:** This includes those platforms that allow the user to create, upload, modify, access information using its services.
- **Significant social media intermediary:** This includes those platforms that have registered users in India above the threshold as notified by Central Government.

KEY FEATURES OF THE ACT

With regards to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 the following features play a vital role in governing the online content being circulated.

- Due Diligence by the intermediaries:
 - Informing the users about the rules and regulations and make people aware about its privacy policy.
 - Inform the online content consumers that in case of non compliance with the guidelines the intermediary shall hold the right to terminate the access to the services that it offers.
 - On receiving a notice, the intermediary shall have the power to remove the infringing content within 36 hrs of its receipt as held under *Super Cassettes vs Myspace*⁴.
 - Take all necessary measures in order to secure its computer databases.
 - Provide within 72 hrs any lawful information that is required by the Government body in order to investigate any cyber security activity.
 - Retaining the information of the user for a period of 180 days after the cancellation or withdrawal of registration which was collected at the time of registration.
 - The intermediary is duty bound to report any data breach or cyber security threat to the Indian Computer Emergency Response Team (CERT).
- **Grievance Redressal:** The intermediary should post on its website the contact information of the Grievance Officer and also the mechanism which can be followed by the victim to get his issue resolved in an efficient manner.
- **3 Tier Grievance Redressal Mechanism:** A tiered mechanism needs to be followed in order to address the complaints in a more efficient manner.

⁴ (2011) 48 PTC 49

- Self-Regulation by the content providers
- Self-regulation by the self-regulating bodies of the publishers headed by a retired judge of the Supreme Court, a High Court, or an independent eminent person from the field of media, broadcasting, entertainment, child rights, human rights or such other relevant field, and have other members, not exceeding six, being experts from the field of media, broadcasting, entertainment, child rights, human rights and such other relevant fields.
- Code of Ethics for digital media publishers: The new code lays down a set of rules that needs to be followed by the online content providers like improving accessibility for online content for the disabled persons and classifying content as age restricted wherever the need is felt.
- Blocking of content in case of emergency: In the case of emergency no delay shall be made if the content violates the Section 69A of the IT Act, 2000. If the Authorised officer finds any content that is not in line with the said provision then he should immediately forward the particulars of such violation to the Secretary of Ministry of Information and Broadcasting. If the Secretary of Ministry of Information and Broadcasting feels that it is necessary to block the online content then he/she should issue a directive which shall lead to interim action taking against such content provider without giving him/her a chance of hearing.
- Guidelines Online content: Certain guidelines must be followed in order to classify the content being transmitted online like general guidelines must be drafted for online content like movies and web series and issue specific guidelines which address the specific issue and also the redressal of the same.

CONCLUSION

Pandemic has brought us to staying indoors and also adopting the medium of watching online content. In pandemic we also saw a rise in the users and an increase in the watch time. This also led to a rise in the crimes being committed online. Hence the government brought in the new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021) in order to streamline the procedure in which the disputes in the online sphere are addressed. This act also lays down the need for classifying certain content as age restricted and also introduction of parental guidance so that the children are safe from having access to inappropriate content being circulated online. Still the government falls short on one aspect of law that is Right to Privacy. The new rules allow the intermediary to break the wall of encryption

to know the First Originator of the message when asked by the governing authorities to do so. This was pointed out by Twitter that this will lead to Freedom of Speech and Expression and Right to Privacy is henceforth automatically curtailed.