SEXUAL PRIVACY AND ITS VIOLATION: A DESPARATE NEED FOR LEGISLATION

Written by **Raghav Kansal* & Arnab Chakraborty****

* 2nd Year BA LLB Student, National Law University Odisha

** 2nd Year BBA LLB Student, National Law University Odisha

ABSTRACT

In 2017, the judgement passed in the case of Justice K.S. Puttaswamy (Retd) v UOI which held that Right to Privacy shall come under the purview of Right to Life under Article 21 of the Constitution of India had created a massive impact on the policies of both the Government and various other private entities and how they function and handle sensitive personal information of the citizens and the users or subscribers of their services respectively. What has gone largely unnoticed and has not nearly received as much attention as it should have done was the petition filed by the NGO Prajwala seeking a change in the policies and the approach of both the government and private organizations and intermediaries with respect to dissemination and dealing with videos and images containing sexually explicit content such as rape/gang-rape (called sensitive and private information) of women and children. The laws that currently exist deal with the circulation of images and videos of pornographic content but no express provision for those data containing very sensitive private information in the Information Technology Act, 2000 and thus can't be classified as a cyber crime.

Perhaps for the first time any cognizance of this alarming issue was taken by the Hyderabad- based NGO Prajwala which wrote a letter to the Chief Justice of India, following which the Supreme Court took a suo moto action. After the hearings and proceedings, several directions were given to the government regarding the setting up of a vigil mechanism and portal for lodging complaints and seeking help. The intermediaries were also directed to modify their policy of privacy both with respect to the rights speech and expression and also for the rights of those whose videos in sexually compromising positions are created and circulated.

The main points of discussion in this paper shall be first; the revolution in privacy matters brought about by the Puttaswamy judgement; second, the failure of the government or any other organization to take any action before the letter was sent to the Chief Justice of India by Prajwala, third; the lack of appropriate and specific laws for such a sensitive subject in any statute in India, fourth; the Directions given by the Supreme Court and the recommendations of the appointed committee, and lastly; how have the policies been implemented and have there been any substantive changes.

INTRODUCTION

REVOLUTION IN PRIVACY MATTERS BROUGHT ABOUT BY PUTTASWAMY JUDGEMENT

Protection of privacy has always been a source of major concern for citizens and the State. As enshrined in Part. III of the Constitution, fundamental rights are those rights that every individual possesses and it can be enforced against the State. Violation of such rights lead to penal consequences. In recent years, online data sharing has gained momentum and the entire country is gradually trying to embrace the fact that data sharing may eventually lead to breach of privacy. The Aadhaar framework was the antecedent to a series of litigations where dispensing or sharing of personal data with the Government was questioned. It was only after the Puttaswamy judgement surfaced that privacy was considered to be an essential element of human dignity. If we roll back the years, we shall see that in M.P. Sharma [i]and Kharak Singh[ii], privacy was not attributed the status of a fundamental right. Justice Chandrachud was unambiguous when he stated that intrinsic value, autonomy and community value are three cardinal aspects of human virtue. They cannot be completed alienated from a person's life and any right which is inherently tangled with human existence has to come under the ambit of fundamental right. The very essence of fundamental rights is to ensure a certain degree of vigil on legislation as also to assure people of their basic human dignity.

Through the Puttaswamy judgement, various privacy breach tests came into the picture. While the majority opinion primarily banked upon the "proportionality" test, the dissenting judgement was driven by "compelling state interest" test. Proportionality test is a set of rules determining the necessary and sufficient conditions for limitation of a constitutionally

protected law to be constitutionally permissible.[iii] In other words, there needs to be a proper relation between the importance of achieving the proper purpose and the social denotation of averting the limitation on constitutional right. Precisely, four elements of judicial review standard were laid down in this judgement - legality, legitimate objective, proportionality and procedural guarantees[iv]. If we look into these prerequisites, what we can derive is that procedural guarantees are extremely subjective. Thus, there needs to be a ground rule or basis to which the judiciary should ideally stick while reviewing the legislation which might breach individual privacy. It is impractical to say that the State will have zero interference when it comes to sharing of one's personal data with a State appointed data bank. However, it is upon us to decide the degree of State's interference in such matters. The State has the power to impose reasonable restrictions on Fundamental Rights but under the pretext of reasonability, we cannot allow the State to impose upon us a legislation which fails to protect personal data of the people.

Whether Right to Privacy is only enforceable against the State is also a question which needs to be emphasized upon. Akin to other Fundamental Rights, this right shall also be enforced against the State. However, there are numerous private stakeholders involved in the form of online intermediaries such as Whatsapp, Facebook etc. Hence, it becomes important to monitor their activities to a considerable extent in order to ensure the motive of having Right to Privacy as a fundamental right is achieved.[v] The State has a responsibility to protect this right and it has to play the role of a mediator between private intermediaries and the citizens. There have been instances when private intermediaries have failed to protect personal data of individuals. Interception of messages or any form of communication is violation of Article 21. The Information Technology Act, 2000 has provisions to keep a vigil on privacy breach but at the same time, these provisions have proved to be inadequate in multiple situations. When the State introduced the Aadhaar bill in the Parliament, it was proposed to be a unique identification document which shall be used for all identification purposes in the long run. At the same time, this would ensure uniformity in documents of identity, that is, instead of using voter cards, driving license or pan cards as identity proof, the Aadhaar card should be considered a legitimate identity proof all across the country. This would safeguard the welfare interests of the people and maintain fluidity in functioning of the State. [Read IT Act relevant provisions]

Identity theft is a cause of serious concern in a world where social media and online resources have created a buzz among the people. Section 66C of the Information Technology Act addresses this issue by laying down the penal consequences arising out of dishonest use of electronic signature, password or any other unique identification feature.[vi] The Aadhaar Act is an attempt to prevent identity theft but the legitimacy of the scheme has been seriously questioned in the K.S Puttaswamy judgement. In a bid to protect someone's identity, large amount of personal data is being compromised and such data are being used to channelize the person's choice or interest for commercial benefits. Data protection in public domain is a very serious issue and there has to be more effective statutory guidelines and State measures to ensure people do not fall prey to profit generating strategies of online intermediaries.

Section 43A of the Information Technology Act attaches liability to a body corporate which fails to protect sensitive personal data through reasonable security procedures[vii]. Rule 3 of the SPDI Rules[viii] also form a strong abutment to the concerned section. Again, the line of distinction between sensitive personal data and personal data is so fine that it becomes necessary to construct a threshold for grading data as sensitive. Banking information, electronic signatures etc. are a few subjects that constitute sensitive data, breach of which can lead to wrongful loss. In brief, online intermediaries need to keep themselves aware of the data protection policies laid down in the Information Technology Act along with the privacy protection right of citizens derived from the Indian constitution.

The Aadhaar Act is an attempt to fine tune and simplify the identification process of citizens of the country. However, there should be stringent guidelines and measures to prevent misuse of data shared by the people as that would portray misplaced trust and the Government will be pointed fingers at.

FAILURE OF THE GOVERNMENT AND ALL OTHER ORGANIZATIONS PRIOR TO THE PRAJWALA CASE

Ms. Sunitha Krishnan, the Hyderabad-based social activist who runs the NGO Prajwala, posted two videos online on YouTube which showed women being raped and sexually assaulted. She posted those videos after blurring out the faces and body parts of the women who were victims of the heinous crimes while she let the faces of the perpetrators of the crime

remain visible. This was done to launch the campaign called "Shame the Rapist". The Right to Privacy was recognized as a fundamental right as a part of Right to Life[ix] as late as in 2017 via the historic judgement in Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors.[x] The right to live with dignity also falls within the scope of right to life. The campaign launched by Ms. Sunitha Krishnan, although with a socialistic intention, did not stop the circulation of the unedited versions of the two videos which she had received, that is, the ones in which the faces and the body parts (genitals) of the victims were visible thereby making them identifiable. This wasn't the first instance in which the video of a woman being raped was circulated online. There seems to be an entire market for such videos[xi]. Whether or not the right to privacy became a fundamental right in essence until 2017, the Information Technology Act, 2000 and the cyber laws of the country have no substantive provisions with regards to the collection and circulation of videos/images or any content which shows the victim being raped, sexually harassed and/or assaulted.

The Nirbhaya incident occurred in December, 2012 and to this date the identity of the victim has been kept confidential. Keeping the identity of the victim secret has been a norm and the duty of the courts and other law enforcement agencies. The courts and the police are required to follow this principle as it was laid down by the Supreme Court in the cases of Delhi Domestic Working Woman's Forum v Union of India[xii] and State of Punjab v Gurmit Singh[xiii]. In the case of Chairman, Railway Board v Chandrima Das[xiv], it was held by the apex court that "rape" amounted to a violation of the fundamental right of the victim guaranteed by Article 21 of the Indian Constitution. If the heinous crime of rape by itself violates the fundamental right of the victim, and since there is substantive precedent which provides that the identity of the rape victims shall be kept confidential even during court proceedings and also in the orders passed by the court, it becomes imperative that the identity of the victim shall be protected and there must be measures to stop it from being leaked via any media.

The letter written to the Supreme Court by Prajwala, dated 18/02/2015 titled "Videos of Sexual Violence and Recommendations"[xv] was the first time any call for the change in the existing laws or the lack of it regarding the privacy rights of the victims of rape and sexual assault with respect to the videos being circulated via social media platforms had made. The Supreme Court took cognizance of the matter and there was a suo moto action in which the

NGO, the government and various social media platforms were issued notices to appear for hearing.

After it was decided that the matter shall be heard by the apex court, Ms. Krishnan in a statement said that she was receiving videos of women being raped/gang-raped or sexually assaulted from various sources including the victims themselves who wanted her to spread the edited version of their videos in an attempt to secure justice. Ms. Krishnan said that "we need a permanent mechanism to deal with such situations. I cannot become the national registry for all rape videos. Cyber cell does not take suo motu notice of the videos. There should be a complainant but sadly nobody wants to become a complainant as a million questions are asked[xvi]."

In the letter to the Supreme Court by Prajwala, it made six suggestions for both the short-term and long-term solution to the problem of spreading of videos showing rape, gang-rape and sexual assault.[xvii] The suggestions were as follows:

There must be a CBI (Central Bureau of Investigation) probe into the videos and all the findings shall be made public.

A Task Force on Sexual Crimes should be set up under the Ministry of Home Affairs (MHA) and it should also focus on technology driven sexual crimes.

There should be a public-friendly mechanism to report such videos. The mechanism could have a secure e-mail id and a toll free number to ensure there is no perception of threat.

A National Sex Offenders Register shall be maintained of convicted sex offenders in the form of a registry. It could contain information of those convicted for eve-teasing, stalking, rape, molestation and other similar offences.

Tie-up of the Ministry of Home Affairs with YouTube and WhatsApp to curb the dissemination of videos containing material which is offensive and related to sexual crimes and also that penal action can be taken against the offenders.

Specialized training of senior law enforcers on issues relating to sexual crimes and cyber space and in use of other technology to tackle concerns from social media and other technology enabled applications such as YouTube and WhatsApp.

The Supreme Court recognizing the failure of the state police departments in apprehending the accused instantly accepted the first suggestion made by Prajwala, and asked for a notice to be issued to the CBI Director to start investigating into the matter with immediate effect and also asked the all the authorities and official to effectively co-operate with one another. This directive by the court became the first definitive involvement and enquiry into such matters by any real authority in India.

INSUFFICIENT LAWS FOR DATA PROTECTION

The introduction of Information Technology Act in 2000 led to the dawn of a new aeon with respect to online data protection. Aadhaar was nowhere in the context when the Information Technology Act was enacted, but the need to have statutory provisions to protect online personal data was felt. Although, the Act as a whole did assure the citizens of protecting their personal data, there was hiatus in the provisions of the Act which needed to be addressed.

The amended version of the European Union General Data Protection Regulation has become applicable from 25th May, 2018. The Aadhaar Scheme makes it mandatory for foreign citizens who are taxpayers in this country to also obtain an Aadhaar card along with the already in place PAN cards[xviii]. Hence, the obvious question that arises is whether the provisions of GDPR are applicable against Indian corporate bodies? There is a high degree of ambiguity prevailing in this context. The legal experts have opined that the provisions of EUGDPR shall be enforceable against Indian companies if it is filed before the Indian court through the Civil Procedure Code. The GDPR is a tried and tested compilation of data protection regulations whereas the Information Technology Act is a fairly young statute of data protection in India. Also, there is limited provisions in the statute for sheltering of "sensitive" personal data. Hence, the IT Act had to be supplemented with the Sensitive Data Protection Rules[xix] in 2011 in order to assure the citizens that their "sensitive" personal data are in safe custody.

In absence of a well-versed data protecting regime in India, the private companies are forced to face the brunt of the people at large. Huge investments are involved and also the fact that they are accountable to the shareholders and customers for any negligence on their part makes them all the more willing to have a GDPR-like data protection regime which includes provisions for protecting all kinds of personal data. The Indian Penal Code also does not have a dedicated section for data privacy breaches. Hence, liability for such breaches must be

inferred from analogous crimes. For instance, Section 403 of the IPC imposes liability for dishonest misappropriation of "movable property" for one's own use.[xx] Lack of potent privacy protection regulations has created a dent in the Foreign Direct Investment sector of the economy. Trade regulatory bodies such as the National Association of Service and Software Companies (NASSCOM) has tried to improve the conditions by creating centralized databases of the employees for the IT services and the BPO sector. Also, many BPO service providers have adopted self monitoring policies to reduce the risk of misuse of personal data. [xxi]

Internet banking and online shopping has become rampant in today's world. In order to facilitate customers and ensure smooth functioning, bank account details and other personal data are often asked for by these websites. Customers are often hesitant while giving away personal details fearing misappropriation of data. Justice B.N. Srikrishna Committee submitted a draft Personal Data Protection Bill in 2018 to form the framework for India's data protection laws, prescribing how organizations should collect, process and store citizen's data.[xxii] Chapter VIII of the Bill talks about localizing data before transferring personal data outside India. To meet this provision of the bill, large scale investments would be necessary. This would eventually make India an undesirable market to set shop in. Even for the existing players in the market, they will have to collocate sufficient resources to satisfy this provision of the bill. The bill also intends to improve transparency and accountability by establishing a data protection authority to store data and the authority can be sued and sue in their capacity of the same.[xxiii] However, this shall create autonomy and arbitrariness on the part of the Central Government since Section 98 of the bill[xxiv] gives unfettered power to the government and any direction issued by the Government shall be considered binding on the authority.

DIRECTIONS GIVEN BY THE SUPREME COURT AND THE RECOMMENDATIONS OF DR. AJAY KUMAR COMMITTEE

The Government of India (GoI) suggested the setting up of a committee with Dr. Ajay Kumar, the then Additional Secretary of the Ministry of Electronics and Information Technology, for the review and reform in the existing laws and mechanism to deal curb and appropriately handle the circulation of those videos depicting rape, gang-rape and sexually violent/explicit content so as to protect the identity and the reputation of the victims.[xxv]

The apex court directed the committee to meet on a regular basis and that after it submitted its report, the court asked the chairman of the committee and the learned counsel for all the parties involved to take instructions from their clients as to whether they are satisfied with the findings and recommendations of the committee or not.[xxvi]

Some of the proposals and the recommendations with respect to them as submitted by the committee to the court are as follows[xxvii]:

The search engines should expand the list of words which may be possibly used by a user to search for child pornographic (CP) content and this list should also cover the words for rape/gang-rape (RGR) content as well. The words should also be in Indian languages and vernacular search.

A cell must be set up either under the CBI or under the aegis of the MHA to deal with these crimes specifically. A hash bank be created for RGR content, formulation of specific parameters for indentifying RGR content and its expeditious removal and that the hashes so generated shall be under the custody of the proposed cell who will seek to prosecute. There must also be a centralised reporting mechanism, preferably with the CBI for reporting and receiving any information regarding the circulation of any videos/images containing CP/RGP content. It was also proposed that the GoI, search engines and the various Content Hosting Platforms (CHPs) shall work together to create a mechanism for proactively identifying and removing CP/RGR content and that technology similar to the Project Arachnid Crawler be used for Indian CP/RGR content specifically.

An online portal and a separate hotline to be set up for anonymous reporting of instances of circulation of CP/RGR videos. There shall be authorised entities to receive complaints, verify the objectionable content, initiate take down and to register FIRs (First Information Reports) and to initiate prosecution accordingly. In case the CBI is interested in handling the matter, the local police shall play a passive role. A team for immediately reviewing the tips given and subsequently communicating with service providers/intermediaries shall also be formed. A tipper list of certain NGOs shall be made and that the GoI shall act expeditiously on the information provided by those NGOs without delay.

The GoI should form regulations for reporting of identified CP/RGR content, it should ensure that those search engines that don't implement URL blocks for identified CP/RGR content start a similar process, human intervention by either the government or the its authorised NGOs to identify CP/RGR content. The personnel involved shall be trained and continuously monitored and reviewed using the funds allocated by the government. GoI/CHPS/search engines shall look to sensitize and create awareness among the judiciary, law enforcement agencies and prosecutors to mitigate the menace of CP/RGR dissemination.

There is a need for development and research on Artificial Intelligence (AI)/Deep Learning (DL)/Machine Learning (ML) techniques for identifying CP/RGR content at the time of uploading itself. Existing technology such as PhotoDNA, Video hashing and others shall be used till new and more efficient technology is developed. The AI/DL/ML tools to be tested in real time. The GoI and CHPs to engage the services of suitable experts to develop DL/ML technology to identify RGR content.

Content removal process for RGR should be as expeditious as it is for CP. CHPs and search engines to have a specific link for reporting CP/RGR content and the same shall be displayed more prominently to the users

CONCLUSION

The Aadhaar Act can be termed as a positive move considering the Government's attempt to address the welfare interests of the rural people, providing subsidies etc. However, the Government needs to ensure safe custody of personal data. Thus, even though the idea of Aadhaar is applauding, its implementation is severely questioned. Including Right to Privacy under Article 21 is an endeavour to further safeguard citizens' interests. K.S. Puttaswamy v. Union of India has become a landmark judgement by virtue of its impetus to protect sensitive personal data.

In order to bulwark private data, the Government should come up with legislations which impose strict penalty on the entities found guilty of breaching personal data. The European countries have the GDPR to protect personal data of their citizens. Even though the Information Technology Act, 2000 has been able to reasonably curtail the number of data

privacy breach incidents, there is no provision for protection of "sensitive" personal data. This is an issue which needs immediate attention, because India is already in an unsteady economic shape and having a weak data protection regime does not help the cause in any way, whatsoever.

The Puttaswamy judgement was a historic one which has changed the way privacy and data protection is being viewed as now in India, both by the Government and the private bodies. The outcome of the case by Prajwala is historic in no less way as the changes it has brought about, at least in the form of the promises by the Government both on an individual level and in coordination with private entities are revolutionary. The most notable implementation of any of the proposed solutions by the Dr. Ajay Kumar committee is the setting up of the "Cybercrime Reporting Portal"[xxviii] under the National Mission for the safety of women by utilising Nirbhaya funds for the reporting of cybercrime related to Child Pornography, Rape/ Gang-rape content. This portal has the facility of reporting anonymously as well for the safety of the victim/complainant. As suggested, this portal functions under the care of the Ministry of Home Affairs. The directions given by the Supreme Court to the Government and other parties, closely resonates with the giving of directions in the case of Sabu Mathew George v Union of India and Ors[xxix], in which search engines and intermediaries were asked to monitor, takedown and also act upon complaints against the display of content related to Pre-natal sex determination of unborn children. Such directions and obligations imposed by the court makes the intermediaries liable to comply, as a failure to do so may result in a contempt of court. Granted that right to privacy per se was recognised as an important aspect of Right to Life under article 21 of the Indian Constitution very recently, but an affirmative action to curb the spread of videos containing sexually explicit content has been taken after a long time of living in a grey area where there was no consensus among the authorities as to what the solution to the problem could be. The directions of the apex court are welcomed and it is expected that all proposals will be made good by the stakeholders as has been promised.

REFERENCES

[i] M.P Sharma and ors. v Satish Chandra , 1954 AIR 300

[ii] Kharak Singh v. State of U.P, AIR 1963 S.C 1295

[iii] K.S Puttaswamy v. Union of India, 2019 1 S.C.C 1

[iv] Indrastra, *An Analysis of Puttaswamy: The Supreme Court's privacy verdict*, November 18,2017, https://medium.com/indrastra/an-analysis-of-puttaswamy-the-supreme-courts-privacy-verdict-53d97d0b3fc6

[v] Jaideep Reddy, *Right to Privacy: SC's verdict on KS Puttaswamy case is landmark, but raises five interesting law and policy issues*, April 23, 2019, https://www.firstpost.com/india/right-to-privacy-scs-verdict-on-ks-puttaswamy-case-is-landmark-but-may-raise-few-law-and-policy-issues-3988913.html

[vi] Information Technology Act, § 66C (2000)

[vii] Information Technology Act, § 43A (2000)

[viii] Sensitive Personal Data Information Rules, Rule 3 (2011)

[ix] INDIA CONST. art. 21.

[x] K.S Puttaswamy v. Union of India, (2019) 1 S.C.C 1

[xi] Aparna Bhat, 8:26 pm, 27-07-2019, https://www.indiatoday.in/india/story/rape-videos-online-sunitha-krishnan-shame-the-rapist-campaign-mms-clip-248260-2015-04-13

[xii] Delhi Domestic Working Woman's Forum v Union of India, (1995) 1 S.C.C 14

[xiii] State of Punjab v Gurmit Singh, (1996) 2 S.C.C 384

[xiv] Chairman, Railway Board v Chandrima Das, AIR 2000 S.C. 998

[xv] In re:Prajwala, SMW (Crl.) No(s).3/2015

[xvi] https://www.indiatoday.in/india/story/rape-videos-online-sunitha-krishnan-shame-the-rapist-campaign-mms-clip-248260-2015-04-13, 8:31 pm, 27-07-2019

[xvii] *id.* At 15

[xviii]Rodl and Partner, "*Indian Data Privacy Laws and EUGDPR*", May 24, 2018, https://www.roedl.com/insights/india-eu-gdpr-data-privacy-law#current

[xix] *id.* At 8

[xx]Manjula Chawla, *Overview of Data Protection Laws in India*, http://www.ehcca.com/presentations/privacysymposium1/steinhoff_2b_h1.pdf

[xxi] *Id*.

[xxii] The Personal Data Protection Bill, (2018)

[xxiii] Ananya Bhattacharya, *India's first data protection bill is riddled with problems*, July 30, 2018. https://qz.com/india/1343154/justice-srikrishnas-data-protection-bill-for-india-is-full-of-holes/

[xxiv] The Personal Data Protection Bill, § 98 (2018)

[xxv] In Re: Prajwala, SMW (Crl.) No(s).3/2015

[xxvi] *Id*.

[xxvii] *Id*.

[xxviii] https://cybercrime.gov.in/cybercitizen/home.htm 8:50

[xxix] Sabu Mathew George v Union of India and Ors, WP No.341/2018.