IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THREATS OF COOKIES & PRIVACY CONCERN

Submitted by

KRITI MAKHARIA

BHARATI VIDYAPEETH (DEEMED TO BE UNIVERSITY)

NEW LAW COLLEGE

CYBER LAW

ABSTRACT

'I visited a diabetes awareness site and it asked me whether I will accept all the cookies, is that a trick question?'

Well, when we talk about cookies, the first thing to cross our mind is a treat of chocolate and butter crunch. But in virtual world, cookie is more than a dessert menu and have to be chosen carefully. We might have noticed that whenever we enter into a website it asks for permission to grant access to cookies, it is nothing but a tiny text file stored in the browser of our devices used for collecting our search or interest data. It remembers the interests and likes of the users. In a layman term, it is a memory chip of the user's information about their likes and wants which uses the data to personalize the user's experience. The website uses the said data to regulate the advertisement of the products according to our interests. A device cookie known as the browser, i.e., the internet or web and also known as HTTP cookies, stores data related to the login credentials, or shopping list or web experiences and cookies makes the working and regulation of such data smoother by providing the exact data of the user's choice. But with the rising AI advancements also increases the threat of potential cookie problems. When we store our data or login credentials to a site then the data is stored in the browser which may also include

the payment information, address of the users, passwords and etc. can be used cyber attackers and fraudsters and can infringe our right to privacy by unlawfully authorising such data. This paper talks about the types of cookies and security concerns faced in today's scenario. Additionally, it lays down the various legal aspect which is needed in improvement of cybersecurity.

KEYWORDS

Digital data, cookies, data privacy, cyber security, DPDP Act 2023

INTRODUCTION

With changing time, innovation and AI (artificial intelligence) plays a very crucial role in every individual's life. With the rise of cyber world, cookies play a very prominent role in tailoring an individual's interest. These are the data files which is stored in the browser of one's computer and activates or track the choice of a man. As we know that the today's generation is the slave of technology. If we want to purchase anything, we can do that from the comfort and leisure of our home from a single click, and the goods will be delivered to our home. Based on our last purchase and recent visits to site; company uses the specific data to customize the products according to our choice. In the very same way with every personalization on any site the cookie remembers the data, for instance saving the card details. Furthermore, there are different varieties of cookies available on our website such as- necessary cookies, zombie cookies, third-party cookies, session cookies, etc.; in which some are privacy intrusive and some are not. Since the society has developed from where the man with power use to be the head of the society to the laws protecting the rights of the weaker section of society shows the adaption with the evolution of time. In the very similar way, the development of technology also has its own short-comings. With the advancement of information technology (IT), human being has to pay a price of it, which is related to their privacy rights.

TYPES OF COOKIES –

- SESSION COOKIES / TEMPORARY COOKIES – These cookies are generally used on shopping sites or for e-commerce. These cookies are active when the users visit the website and record their action and gets deleted when the users log out. They navigate through the users' activities on the website.
- FIRST-PARTY COOKIES – these cookies help in providing good experience to the users, by remembering their language setting or other such preferences set by them when they visit the domain on the address bar.
- PERMANENT COOKIES/ PERSISTENT COOKIES – these cookies are saved permanently on the browser such as the log-in details of the users so that when the user log-in next time into the browser the said website will remember their credentials. It is also said that the login credentials should be changed after every 12 months for safety purposes[1].
- FLASH COOKIES – These cookies are stored in a separate Adobe file. These super cookies are stored permanently on the devices even after all the cookies are disabled from the device and can be used to recreate deleted HTTP cookies. These cookies are no more in use as it creates privacy concern of the user's data.
- ZOMBIE COOKIES – they are different type of flash cookies which gets automatically recreated after they are deleted. These cookies are very hard to detect and can often cause privacy concerns by creating malicious software on the user's device[2].

COOKIES & PRIVACY

A small text file stored in our browser was developed first time in 1994 by Lou Montulli. Cookies was not widely known at the time when Montulli developed it with John Giannandrea. As an employee of e-commerce company called Netscape Communication, he developed the cookies from 'Magic Cookies' for the purpose of storing and communicating data with users. As we know cookie stores the data in the browser. But as some cookies are privacy intrusive like third-party cookies also known as tracking cookies. It collects the data every time a user visits a website and sends it to the website which created that cookie, for instance a user visiting an educational site can see the ads of different products by different companies; this can be done when the company uses the previous data collected by different cookies for the selective advertisement to attract the customers to their products by enabling third-party cookies. These data stored in the web can also be used by cookie hijackers (cookie hijacking or cookie

[1] What are Persistent cookies, cookie 101. https://www.cookieyes.com/knowledge-base/cookies-101/what-are-persistent-cookies/#:~:text=Persistent%20cookies%20or%20permanent%20cookies,they%20close%20a%20web%20browser.

[2] What are Zombie cookies, cookie serve. https://www.cookieserve.com/knowledge-base/website-cookies/what-are-zombie-cookies/#:~:text=These%20cookies%20are%20stored%20in,personal%20information%20without%20your%20consent.

tossing) infringing the privacy rights of an individual enshrined under Article 21 of the Indian Constitution.

As Marlon Brando said, "Privacy is not something that I am merely entitled to, it is an absolute prerequisite."

Cookies and privacy go hand-in-hand, and is a part of very heated discussion nowadays. With ever rising cybersecurity threats, people's right to privacy as a fundamental is right is getting breached. With numerous cases of infringement leads to the rising concerns for stringent laws to deal with it. Lately, during an epidemic of COVID-19, government provided vaccination to its citizens, and the data of vaccination with other related personal information such as address, e-mail, PAN number, mobile numbers, etc., of 81 crore people was leaked and was made available on the dark web[3]. As such huge data related to a person's personal information increased the concern for more safety measures.

In India we do not have a specific legislation to deal with privacy right or with the usage of cookies. The supreme court (SC) has recognized right to informational privacy under Article 21 of Part III of the Indian Constitution[4] in a landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.,[5] which laid the foundation of protection of data of an individual in the aspect of their privacy. But there is no laws or judgements related to functioning of cookies. As cookies is not regarded as personal data in India, companies' plants various unnecessary cookies to extract data. It leads to unauthorised use of data and the data principal anonymization is exposed. The existing legislation related to the breach of data is insufficient and India needs more stringent laws while dealing with cookies and other cybersecurity issues.

INSUFFICIENY OF EXISTING LEGISLATION

Indian Contract Act, 1872

Whenever we visit any website, we are asked to accept certain cookie policy or reject it, these are nothing but the terms and conditions laid down by the websites binding us into a legal contract. However, in India there is no aspect of privacy in cookie policy since cookie consents are not treated as personal information. Due to which the websites wilfully disobey this policy and implant an arbitrary cookie into our website and can manipulate our choices. This consent can also be regarded as unconscious consent and will amount to void contract. But as there is no specific legislation protecting the consent of the users as personal information then their rights are easily violated.

[3] HINDU, The Hindu Business Line, 2023. https://www.thehindubusinessline.com/news/covid-test-info-over-81-crore-indians-reportedly-breached/article67477098.ece. Jacob Puliyel v. UOI & ors. AIR 2022 SC 533.

[4] Art. 21 of Indian Constitution.

[5] Justice K.S. Puttaswamy v. UOI AIR 2017 SC 4161.

Information Technology Act 2000

Since the advancement of technology, IT act 2000 was amended in 2008 and added various rules to protect the SPDI, notified by the government in 2011 for the companies and the corporate sector to adhere by it. But as the rules are related to the sensitive personal data or information, there is no specific legislation related to cookie in it. SPDI only includes a sub-category of personal data, i.e., passwords, financial & biometric information, health related information. The company can always argue their way out of the liability by taking out some technical glitch in the said definition. We cannot even regard cookie as a 'computer virus' since cookies are not always malicious in nature and is also for the benefit of the users.

ENACTMENT OF DPDP ACT 2023

With changing time of technology from telephones to smartphones and continuous advancement of artificial intelligence the need to secure the rights of an individual was becoming very prominent. So, to deal with this DPDP Act 2023 came into force, which is passed by the Parliament but is yet to be enacted.

Digital Personal Data Protection Act,2023 (11 August 2023), is the first comprehensive legislation regarding the protection of digital data of a data principal based on the principal of transparency and accountability. It also applies to the data obtained from the Indian residents by the organisation residing outside India. The data should be obtained by the data fiduciary through valid consent given by the data principal. Every principal of the data has the right to access their data and to delete their data according to their need. It has an opt-in process that requires granular consent. The Data Protection Board will act as the regulatory body for dealing or accessing the data prom the data principal.

HOW THE CURRENT LEGISLATION IS DIFFERENT FROM OTHER FOREIGN LAWS

What is GDPR?

The general data protection regime was enforced by the European Union to protect their citizen's personal information from being vulnerable to the threats of cybercrimes. It sets out the unified rules and regulation imposed throughout the world if they are dealing with any data localised in the territory of EU (the DPDPA 2023, has adopted this measure in our system). It limited the use of data by setting out the rules for which it can be accessed and made the use of data transparent and accurate.

DIFFERENCES

- GDPR holds the statutory obligation on both the data processor and the data controller unlike the DPDP Act 2023 which holds the data fiduciaries liable for the act of the data processor solely. There is no difference between the SPDI or personal data in India, all data which is reveals a person's identity will be regarded as personal dealt under DPDPA 2023.

- GDPR laid down specific instruction to be followed by data users if collected outside the territorial borders whereas, India has very limited provision dealing with extra territorial data, it is only subject to the information provided to dealers of goods and services, who will qualify as data fiduciary under the Act. India has an opt-in method which helps the business as it does not require a granular consent unlike GDPR.
- Under the DPDP act it states that the data fiduciary can collect data only with the consent of the users and for a lawful purpose. If the collected data is unlawful then the data fiduciary will be held liable for the unauthorised use of data. The data principal can always have the option to withdraw their consent in a lawful manner. GDPR covers for a vast number of lawful purpose than DPDP which includes data processing for contractual obligation or for the interest of data controller.
- Rights related to automated data; data portability is not provided under the DPDPA.
- DPDP Act has enacted a new regulatory body to deal with infringement or leak of any personal information without the consent of the data principal which mainly focuses on penalising data breaches whereas GDPR includes rule making and other administrative functions to protect the data of the individuals.

Since DPDP Act 2023 is not a replica of GDPR, but it is similar to the thought behind the legislation of the same; that is to eradicate the growing cybercrimes in the technological world. Both the Act tries to provide accountability and transparency in the collection of personal data and held the person liable who hampers the right to privacy of an individual.

When we look at this Act it has created two worlds of private and public sector (Government), it has imposed various rigorous legislation when it comes to the data collected by any private legal entity whereas it gives a lot of exemptions to the government when it comes to the processing of data of the citizens (it can be biometric data, address, phone number, etc.) and exempts them from their liability. This Act of 2023 puts more focus on economic and sovereignty of the state rather than the privacy of the people. It boosts the international trade by giving easier way of obtaining consent from the user unlike GDPR which provides very specific regime to be followed by every individual who is dealing with the citizen's data.

JUDICIAL PRONOUNCEMENTS RELATED TO PRIVACY ISSUES IN CYBER WORLD

- Justice K.S. Puttaswamy (Retd.) & Anr. Vs. Union of India & ors[6].

This a landmark judgement which paved the path of privacy as a fundamental right into part III of the Indian constitution. The court under this Aadhaar case held that right to privacy also includes security while dealing with online data. Any data which shows the identity of any person will be regarded as personal data and any unauthorised use of such data will be regarded as infringement of right to privacy

[6] Justice K.S. Puttaswamy v. UOI AIR 2017 SC 4161 (Supra). (Hindu 2023)

u/a 21 of the Indian constitution. The supreme court overruled the previous judgements of M.P Sharma v. Satish Chandra[7] and Kharak Singh v. State of Uttar Pradesh[8].

- PUCL Vs. Union of India & ors[9].

  In this case the supreme court declared that phone tapping without safety measures is a breach of fundamental right of an individual, and further stated that any act of unauthorised use of personal data will violate the fundamental right unless procedure established by the law. It also criticised the government for failing to take appropriate safeguards in dealing with personal data.

- R.S Raghunath v. State of Karnataka.

  "In this case it was held that IT Act,2000 is a special law enacted especially to deal with IT-related issues and Data protection act is enacted especially to deal with right to privacy, hence, the supremacy of both the act is contradictory"[10].

- District Registrar and Collector v. Canara bank[11].

  The hon'ble court observed that while dealing with personal data if there is no proper guidelines has been laid down for exercising of power and recording the availability of grounds on which the power can be exercised then the entire exercise will be regarded as unreasonable for dealing with the same.

RECOMMENDATIONS

1. There should be clarity regarding the supremacy of laws in the countries. As we know IT Act, 2000 was enacted to deal with the data of the individual and DPDPA,2023 is step towards ensuring the right to privacy of the people, but there is always a contradiction with the prevailing laws, which should be made clear.
2. There should be a specific test of reasonability mentioned to deal with sensitive personal data. It is only decided through judicial discretion and precedent.
3. India is a country where many of its citizens are not aware about the threats related to cookies or are very ignorant in this fast-changing world, which often paves the path for cyber criminals to find their way to blackmail them. To protect them from such crimes; the storage of data-by-data fiduciaries should not be done on consent basis, but on right based model.[12]
4. As India being one of the growing economies, it deals with import and export of large numbers of data throughout the world. So, it should have more stringent policies to deal with the personal data crossing borders to keep the identity of its citizens secure.

[7] M.P. Sharma v. Satish Chandra AIR 1954 SC 1077.
[8] Kharak Singh v. state of Uttar Pradesh AIR 1964 SCR 332.
[9] PUCL V. UOI AIR1997 SC 568.
[10] R.S. Raghunath v. state of Karnataka AIR 1992 SC 81.
[11] District registrar and collector v. canara bank.
[12] Data protection & privacy issues in India
Data-Protection-26-Privacy-Issues-in-India.pdf (elplaw.in)

5. The DPDPA, 2023 should make a clear distinction between the personal data and the sensitive personal data while dealing with it and accordingly measures should be taken.

CONCLUSION

As India has taken a step forward to deal with the budding issues of cookies and privacy still has to work various other distinctive areas as compared to foreign laws. The growing needs of technology at every stance has made humans slave to it. Nowadays a man cannot survive without the AI. With ever good there is an evil; in the same way with every advancement there is a need of protection. The legislation of DPDPA, 2023 is an initiative toward protecting the right of citizens and limiting the right of information in case of private data. As compared to the legislation of European union's GDPR, the current Act of 2023 is less detailed and lacks at various issues but it does give a clear view of how the personal data should be recorded, treated and used by the businesses and provides relief in case of breach and also legalising the use of data by central government in cases of adverse situation such as threat to sovereignty, to maintain public order, in examination of criminal offences etc.