VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

CONSENT IN THE AGE OF DIGITAL INTOXICATION

- Jyotiraditya Baunthiyal & Chandan Daswani[1]

Consent, Autonomy, and Constitutional Foundations

The concept of consent is a foundational pillar of modern liberal democracy, law, and ethics. **H.L.A. Hart** described consent as the point at which law respects an individual's capacity to choose for themselves, even when that choice carries risk or disadvantage. Consent is a fundamental concept that occupies a central position in medical settings, contractual agreements, personal interactions, legal reasoning, and across multiple branches of law, including criminal law, contract law, and constitutional theory. Indian constitutional jurisprudence echoes this view profoundly, which can be observed in the light of the *Right of Personal Liberty* and *Right of Privacy* enshrined within *Article 21 of the Indian Constitution*.

The Supreme Court has repeatedly linked consent to decisional autonomy, holding that the ability to make meaningful choices is an inseparable part of personal liberty under ***Article 21[2]. In K.S. Puttaswamy v. Union of India[3].*** The Court emphasised that autonomy loses its substance when choices are shaped without awareness or genuine control. Consent, in this sense, is not just about formal agreement but about the conditions under which that agreement is formed. A decision is considered ethically and legally sound only if it is informed and freely given. Yet, this bedrock principle is under unprecedented strain in digital environments.

The traditional notion of consent advocates for the ideology that a person has the right to opt to either accept or abstain from a proposed term or condition, yet the contemporary digital web is at a striking dichotomy with the concept. A person encounters a myriad of requests from numerous applications to grant them consent to access that very individual's personal data, for instance, images, contacts, and location etc., and one of the most common yet quintessential for this article being "*Cookies*".

[1] Student at Symbiosis Law School, Pune.
[2] INDIA CONST. art. 21.
[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

Cookies and the Illusion of Choice

Cookies are one of the core areas where *Article 21* of the Constitution is disregarded, and the right to privacy is being legally infringed due to the scarcity of a statutory framework. *Article 21* explicitly emphasizes the necessity and sanctity of the "Right to Privacy", and dictates that privacy is an essential aspect of personal liberty and dignity, and is intrinsic to the entire constitutional scheme; however, when we dive deeper into the actuality of cookies, it would be as clear as a crystal that they are not what they apparently seem to be. Generally, people see them and think that they are just a permission to enter the website, and people turn a blind eye to the fact that this very "permission" is costing them their digital privacy, and the severity of the subject matter can be comprehended by the fact that many people, despite being reluctant to agree to such terms, are compelled to grant their consent reason being the blockaded access to the data they need.

Free Consent Under the DPDP Act: Law and Reality

The DPDP Act, 2023 mandates that the "Data Principal" has the right to accept the circulation of his private information at his "free consent", and currently, the cookie policies being adopted by websites are known to propel the users to give their consent rather than seeking "free consent", as the cookie banners are known to provide only two options, either "Accept All", or "Accept Useful Cookies", which leaves the user with no option but to accept these policies either at their maximum or partial extent.

Essentially, cookies are small code files downloaded to users' devices by the websites they visit. Cookies track visitor activity and provide personalisation, which is generally of two types: *first-party and third-party*. The former are accessible only by the domain that created them; the latter are accessible by all the websites that load a third-party server's code, allowing such third-party cookies to be tracked by websites other than those an individual visits. This feature enables businesses to track the activities of site visitors and collect, process, and manage their personal data. Most significantly, it enables advertisers to target advertisements at the right viewers**.**

Trapping Patterns and Digital Compulsion

The virtual world has become increasingly entangled in a nexus of "soft-traps" being used by websites. Skyrocketing rates of inescapable cookie policies, nudges, clickbait, and dopamine loops are being implemented by numerous websites in an effort to boost their usage, and such

a user interface has become a problem for frequent internet users.There is always a lingering conundrum of clicking either *"Accept all" or "Manage Cookies"*, with no option to avoid getting our internet feeds infested by these websites. Such entrapments pose significant hindrances in academic and research domains, where students and researchers are compelled to accept all cookies encountered on websites they visit, which inevitably impacts their internet experience and recommendations, regardless of their preferences.

When Acceptance Is Not Consent: Empirical Insights

Across the world, it has been widely reported that internet giants manipulate their cookie banners to conceal the "Reject All" option in cookie policies, resulting in a "Accept All" rate of 60-90%[4].However, when users are granted the liberty to evade such policies, they gladly opt for it, as evidenced by a 40-50% decline in the rate once the option is granted.

Empirical data becomes crucial in this context, as it reveals how consent operates in practice rather than in theory. High acceptance rates, therefore, function as indicators of systemic design pressure rather than genuine user approval.

The same fact has been observed by *Josh Koebert* and *Kalleigh Lane*[5]while consolidating statistical data on how many people are aware and willing to sign up for cookies. They observed that *61%* of the American population is not fully confidentin accepting cookies during their virtual journey.

Before examining India's legal position, it is essential to consider how other jurisdictions regulate cookie consent and online tracking. Since digital platforms operate across borders and often adhere to the weakest compliance standards, a comparative analysis helps assess whether consent genuinely protects user autonomy or is merely formal. International frameworks, therefore, provide useful benchmarks for understanding how law can respond when technology itself distorts free and informed consent.

The European Union Approach

In global standards, there does not exist a single global convention or treaty governing the law of cookie management. However, a patchwork of regional and national legislative frameworks exists. The benchmark law against which all data privacy laws are compared is the GDPR. Although the GDPR does not directly regulate cookies as a standalone subject, it

[4] Ignite Video, *Cookie Consent Studies*, IGNITE (n.d.)
[5] All About Cookies, *Internet Cookies Survey*, ALL ABOUT COOKIES (n.d.),

governs cookies insofar as they involve the processing of personal data, which brings tracking, profiling, and consent-based cookie practices squarely within its scope. Under the GDPR, the use of cookies and similar tracking tools is permitted only when it relies on a valid legal basis, typically user consent. Such consent must be voluntary, specific, informed, and clearly expressed, meaning users must be able to choose freely and cannot be compelled to accept tracking just to use a website. Consent cannot be based on pre-selected options, assumed from silence, or obtained through deceptive interface design. The GDPR also grants individuals robust rights, such as withdrawing consent, accessing their personal data, and requesting its deletion, and enforces these rights with heavy fines, making it a strong and effective regime for governing online tracking. The ePrivacy Directive (2002/58/EC)[6] regulates electronic communications, requiring prior user consent for non-essential cookies and protecting confidentiality by limiting tracking and storage of data on user devices. Banners that state "accept or leave the website" are unlawful, and pre-ticked boxes are invalid. European courts and regulators have repeatedly enforced these instruments.

The United States of America

The US does not recognise privacy as a fundamental right in the same way. Laws such as California's CCPA[7] and CPRA[8] provide users with the right to know what data is collected, to opt out of the sale or sharing of personal information, and require transparency through clear cookie disclosures. However, these frameworks largely rely on opt-out consent rather than prior opt-in consent, and they do not expressly prohibit cookie walls or forced acceptance mechanisms. As a result, these mechanisms are weaker in force compared to those in other jurisdictions.

Soft Law and Global Privacy Norms

The OECD Privacy Guidelines[9], being soft laws, are non-binding in nature. However, they have played a major role in shaping global data protection standards. They establish fundamental guidelines that apply to behavioural tracking via cookies, including collection limitation, purpose specification, use limitation, transparency, and accountability. These

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (ePrivacy Directive), 2002 O.J. (L 201) 37.
[7] California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2024).
[8] California Privacy Rights Act of 2020, CAL. CIV. CODE §§ 1798.100–1798.199.100 (West 2024).
[9] Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013).

guidelines emphasise that data should be handled responsibly, collected fairly, and used only for specified purposes. These ideas are directly incorporated into many national data protection laws, making the OECD framework a crucial starting point for global regulation of online tracking practices.

What India can learn from GDPR and CCPA?

The EU's GDPR and California's CCPA offer important lessons for India's changing data protection environment, which is based on the Digital Personal Data Protection Act of 2023. Prioritising user consent, enforcing purpose limitation, and bolstering data subject rights - such as the rights to deletion, correction, and portability - are all features of both frameworks. In order to encourage responsible data stewardship, they also incorporate algorithmic transparency principles, enforce them through independent regulators, and set severe penalties for non-compliance. By guaranteeing greater regulatory independence, more transparent permission requirements, and enforceable rights that strike a balance between innovation and individual privacy, India may adapt these international norms and enable a rights-based digital economy.

Cookie policy and data protection in India: Is the law silent?

As of the contemporary statutory framework in respect to the Indian legal system, the *Digital Personal Data Protection Act (DPDP Act),* which came into force in the year 2023, has been observed to lack statutory regulations in regard to cookie policies implemented by websites, where it has been made quite straightforward and clear to accept these policies while keeping the option to reject such cookies shrouded.

India's comprehensive approach to data protection is intrinsically intertwined with the *Digital Personal Data Protection Act, 2023 (DPDP Act*[10]*)*. The framework establishes the landscape of processing personal data within India's growing digital economy.[11]

Section 6 of the DPDP Act, 2023 grants the "Data Principal", or in layman's words, the person to whom the personal data belongs, a mandatory right over their free consent to such websites, and whether they want to reveal their personal credentials, and any other information to be uploaded and used by such websites, albeit, it is a prima facie fact that the

[10] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE.
[11] Bar & Bench, *Cookie Management Under the Digital Personal Data Protection Act, 2023*, BAR & BENCH (2023)

entire statute despite granting the "Data Principal" complete authority over his consent still does not regulate the cookie policies adopted by the "world wide web" nexus.

The silence on the specific cookie consent provisions within the DPDP Act does not diminish the importance of efficient cookie management. Instead, it necessitates a nuanced understanding of how general data protection principles apply to cookie consent mechanisms. Organisations must navigate this regulatory framework while ensuring compliance with the broader consent and transparency requirements outlined in the DPDP Act. (Bar and Bench, 2025).

How can users protect themselves?

Despite platforms and regulators bearing primary responsibility, users can still enhance control over their personal data by using privacy-focused browsers, installing cookie/tracker blockers, clearing cookies and revoking unnecessary permissions, and relying on password managers with 2FA. They should also audit app and website privacy settings, avoid social login options, use VPNs on public Wi-Fi, and actively exercise their available data rights, such as deletion, opt-outs, and access requests.

Conclusion: Rethinking Consent in Digital Spaces

Cookies might seem only a minor problem,but the same minor problem has the potential to metamorphose into a global security issue, where these very cookie policies can be used by malicious third-party websites to procure user data and manipulate it at their own will.

Additionally, when we examine the contemporary Indian legal stance and statutes, we notice a significant void regarding policies such as those related to cookies, which often go unnoticed due to their seemingly minor nature. So, is the Indian law waiting for some heinous act to take place? Or has the law turned a blind eye to the issue? These questions are neither being addressed nor answered, with hefty statutes being promulgated for numerous national issues;cookies are one of those issues that are left in the dark.

As a result of this very pseudo-consent, users are bombarded by cookie banners on nearly every website they visit, leading to exhaustion and indifference. This often results in users automatically clicking "Accept All" just to access content, without truly understanding or making an informed choice about what data they are sharing.