DELICIOUS OR DUBIOUS: A LEGAL PERSPECTIVE OF 'E–BAKED COOKIES'

- **Kunal Chandriani, University of Mumbai**

One can certainly not deny his hankering for cookies, after all who can resist these fresh baked luscious snacks, isn't it? However, one may probably not find all the cookies to be delicious, especially the ones baked in the internet's oven. It sounds absurd, but if one jogs his memory, this shall certainly make sense. We all live in a dual world where we have a corporeal residence as well as a digital residence. Market places, social gatherings, recreations and professional meetings are merely a click away. Unquestionably the internet has reprogrammed human lives and at the same time has grown into a virtual limb.

Sneak peek into the jar!

A stereotype day in our lives begins with waking up to the Infobahn notifications. As the day proceeds, we happen to explore various web pages, whether out of professional or personal reasons. This is the time when you knowingly or perhaps unknowingly place an order for cookies. Ever remember opening a website and ignoring a dialogue box which says "This website uses cookies"? In any case, there is a need to understand what these cookies are and whether they can be safely consumed or not. A cookie is a pint-sized piece of text file or data which is sent by a website and saved on the user's device while browsing a website. They are processed and stored by the web browser used while browsing[1]. To explain it in elementary terms, cookie is a kind of information which gets stored on your device while accessing certain websites. To capture a practical understanding, one can take the example of online shopping websites. When you create an account, the website asks for your permission to remember your login credentials. These credentials are nothing but cookies. Further, post logging in, you may want to purchase multiple products, where you proceed to add those products to your cart. These products in your cart are examples of cookies. Thus, by its very nature, cookies are harmless and serve essential functions for websites.

Need for a legislation.

Before understanding the legislative piece on the subject, it is indeed pertinent to know the reason behind its enactment. As mentioned earlier, cookies serve an essential purpose for enhancement of the user's experience with a website. However, the fact that websites store certain private data of the user through the use of cookies, cannot be ignored. It further increases the probability of potentially identifying the user without his consent. This indeed raises serious concerns pertaining to breach of privacy. Thus, ***certain countries which have regarded privacy as one of the integral parts of human lives have felt the need to introduce a dedicated legislation to curb any unauthorized collection and use of personal data[2].***

[1] Cookies, the GDPR, and the ePrivacy Directive, GDPR.eu (2019), https://gdpr.eu/cookies/.

[2] Bobbie Johnson, What you need to know about the EU Cookie Law Gigaom (2012), https://gigaom.com/2012/05/25/cookie-law-explainer/.

The Bitter Cookies!

It isn't a thumb rule that every cookie is necessarily a threat to one's privacy. Thus, an overview of different cookies[3] can be helpful for a secured cyber management.

1. **First-Party cookies:** These get placed on your device directly by the website you are browsing. As seen earlier in the example regarding the online shopping websites, the essential features of 'cart' and remembering login credentials are common first-party cookies. These cookies aren't potentially harmful.

2. **Third-Party cookies:** These cookies get stowed on the end user's device, not by the webpage or the website he browses, but by third parties like advertisers. These cookies can track your online activities to help advertisers deliver more relevant advertising.

3. **Flash / Super cookies:** These cookies perform similar functions as an ordinary cookie, but it's an arduous task to trace and delete. They can stay in a user's device even after deleting all the cookies from the web browser. They can track and collect wide array of data of a person browsing the website.

4. **Zombie cookies:** These cookies can instantly recreate when they get deleted. The recovery is possible due to backups saved apart from a browser's ordinary cookie storage.

Needless to say, except from the First-party cookies, the rest are a potential threat to your privacy.

Regulations

Since the present subject pertains to cyber security and privacy management, it is relevant to refer the legislations of technologically-advanced nations. Amongst such nations, the European Union sets out crucial and effective regulations in this regard. The need for such regulations arises from the "Charter of Fundamental Rights of the European Union". Article 8 of the said Charter focuses on protection of personal data. It further places emphasis on fair processing of the collected data and the consent of the user[4].

- **E-Privacy Directive**
  In 2002, the European Union introduced the "Privacy and Electronic Communications Directive" *(2002/58/EC)*, also known as e-Privacy Directive, which dealt with the governance of a number of vital issues connected with confidentiality of information,

[3] Dan Price, 7 TYPES OF BROWSER COOKIES YOU NEED TO KNOW ABOUT MAKEUSEOF (2018), https://www.makeuseof.com/tag/types-browser-cookies-to-know-about/.

4 ARTICLE 8 - PROTECTION OF PERSONAL DATA, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2020), HTTPS://FRA.EUROPA.EU/EN/EU-CHARTER/ARTICLE/8-PROTECTION-PERSONAL-DATA.

management of traffic data and cookies[5]. This Directive was then amended by the new Directive *(2009/136/EC)*, which came into force in May 2011[6]. The amendment brought a number of changes with respect to users' privacy rights and at the same time, 'prior consent' for the usage of cookies was focused upon. This Directive was thereafter commonly known as the "cookie law". However, it should be remembered that a Directive must not be confused with 'Law' or 'Regulation'. These Directives can be understood to be as a base to enact the laws in the respective member countries[7] *(Just like the Directive Principles in the Indian Constitution).*

- **General Data Protection Regulation (GDPR)**
  As enforced in 2018, the GDPR is a law enacted by the European Union on data protection and privacy[8]. It is often noticed that people have a common misconception that the ePrivacy Directive or the Cookie Law has been repealed by the GDPR, which, in fact, it has not. Instead, it can be said that the ePrivacy Directive and GDPR complement each other[9]. The GDPR, like the ePrivacy Directive, places emphasis on obtaining consent for collecting personal data and at the same time, also elucidates the manner of obtaining such consent.

- **Guidelines by the European Data Protection Board (EDPD)**
  With regards to the GDPR, the European Data Protection Board (EDPB) is an autonomous independent European body which aims to secure consistent application of the GDPR. Amongst other functions, it issues guidelines and recommendations for appropriate practices related to the interpretation, analysis and application of the GDPR. On 4th May 2020, the said Board has come up with certain clarifications regarding consent with respect to cookies[10].

- **Legal Precedent**
  Post enforcement of the GDPR, in the year 2019, the Court of Justice of the European Union (CJEU), in a case before it, ruled that; 'explicit consent' is the only form of valid

5 EU PRIVACY AND ELECTRONIC COMMUNICATIONS (E-PRIVACY DIRECTIVE), ELECTRONIC PRIVACY INFORMATION CENTER, HTTPS://EPIC.ORG/INTERNATIONAL/EU_PRIVACY_AND_ELECTRONIC_COMM.HTML.

6 FRANCESCO ALBINATI, E-PRIVACY DIRECTIVE 2009/136/EC EUROPEAN DATA PROTECTION SUPERVISOR - EUROPEAN DATA PROTECTION SUPERVISOR (2016), HTTPS://EDPS.EUROPA.EU/NODE/3100#E-PRIVACY_DIRECTIVE2009-136-EC.

7 EU COOKIE LAW - A RIGHT TO PRIVACY, COOKIEBOT (2019), HTTPS://WWW.COOKIEBOT.COM/EN/COOKIE-LAW/.

8 MATT BURGESS, WHAT IS GDPR? THE SUMMARY GUIDE TO GDPR COMPLIANCE IN THE UK WIRED (2020), HTTPS://WWW.WIRED.CO.UK/ARTICLE/WHAT-IS-GDPR-UK-EU-LEGISLATION-COMPLIANCE-SUMMARY-FINES-2018.

9 COOKIES AND THE GDPR: WHAT'S REALLY REQUIRED?, IUBENDA, HTTPS://WWW.IUBENDA.COM/EN/HELP/5525-COOKIES-GDPR-REQUIREMENTS.

10 ANTOINE OLBRECHTS, GUIDELINES 05/2020 ON CONSENT UNDER REGULATION 2016/679 EUROPEAN DATA PROTECTION BOARD - EUROPEAN DATA PROTECTION BOARD (2020), HTTPS://EDPB.EUROPA.EU/OUR-WORK-TOOLS/OUR-DOCUMENTS/GUIDELINES/GUIDELINES-052020-CONSENT-UNDER-REGULATION-2016679_EN.

consent for processing user data in the European Union. This ruling was with regards to consent required for website cookies and tracking[11].

Compliances

We touched upon the need for the legislation followed by the regulations put forth in place. Thus, it is obligatory to comply with the laws. Even if this isn't a convincing reason to observe compliance, one must remember that the cost of non-compliance, as per GDPR, can soar up to €20 million or 4% of annual global turnover, whichever is higher[12]. To sum up the compliances as specified under the above-mentioned legit substances, the websites functioning from the member countries of the European Union as well as those international websites that cater to the citizens based out of European Union, need to ensure the following norms:

- Each time a user visits a website, he must be informed about the cookies being collected and used, and such a user should also have the option to accept or refuse the same.

- The consent must be free of any conditions.

- Consent based on an explicit affirmative action.

- A pre-ticked checkbox is an invalid mode of taking consent.

- Certain cookies that are considered as 'strictly necessary' need not be consented for.

- Websites must ensure that consent withdrawal mechanism is put in place, which must be as simple as giving consent, which can be exercised by the user at any given time.

- Cookies must be held back by the websites till the time consent is not given by the user.

- The consent must be granular i.e. consent for all the cookies must not be bundled.

- A Cookies Policy which must set out detailed description that notifies customers about which cookies are used, how they're used, what sort of personal data they collect and who they might share that data with.

11 ACTIVE CONSENT AND THE CASE OF PLANET49: CJEU: GDPR & EPR, ACTIVE CONSENT AND THE CASE OF PLANET49 | CJEU | GDPR & EPR, HTTPS://WWW.COOKIEBOT.COM/EN/PLANET49/.

12 ASHLYN BURGETT, THE COST OF GDPR NON-COMPLIANCE: FINES AND PENALTIES - KIRKPATRICKPRICE KIRKPATRICKPRICE HOME (2020), HTTPS://KIRKPATRICKPRICE.COM/WHITE-PAPERS/COST-GDPR-NON-COMPLIANCE-FINES-PENALTIES/.

- Every such communication pertaining to cookies must be communicated to the user in plain and locally understandable language.

- Actions such as scrolling or swiping through a website or similar user activity shall not, under any circumstances, satisfy the requirement of explicit and affirmative consent.

- The websites must maintain records of cookie consent as required.

Global journey ahead

The "California Consumer Privacy Act" (CCPA) has several similarities with the GDPR[13]. ***The GDPR as well as the CCPA are seen as a model data protection law by various nations outside the European Union (EU), including Japan, Brazil, Chile, South Korea, and Kenya.*** While various nations may rely on their own data privacy laws, non-compliance with the EU data privacy laws, particularly the GDPR, is not an option, since Europe is one of the major commercial trade centers and at certain point one may virtually end up being in the EU nations. At the same time, ***it is important to study the data protection and privacy laws of the nations where one anticipates carrying out his activities which may involve information technology and usage of consumer's data***.

13 BIOMETRIC DATA AND DATA PROTECTION REGULATIONS (GDPR AND CCPA), BIOMETRIC DATA PROTECTION (EU AND US PERSPECTIVES), HTTPS://WWW.THALESGROUP.COM/EN/MARKETS/DIGITAL-IDENTITY-AND-SECURITY/GOVERNMENT/BIOMETRICS/BIOMETRIC-DATA.