

COOKIE CONSENT THROUGH THE CASE PLANET 49

Mariam PILISHVILI*

“Information, as we all know, is power. Both collecting and collating personal information are means of acquiring power, usually at the expense of the data subject.”

A. Michael Froomkin¹

1. Introduction

The internet has permeated every aspect of our society. Due to the rapid development of privacy-destroying technology, private sector monitoring, as well as government surveillance, endangers the privacy and protection of personal data.² As a result, we find ourselves in the internet environment, which is monitored by businesses, advertisers, and users of our social networks, together with the state.³ Ant to protect such a fundamental part of mankind, the need for privacy and data protection has long been acknowledged as core values in the modern world.

The EU and the Council of Europe (Hereafter ‘CoE’) have created legal frameworks that guarantee both the right to privacy and the right to data protection. The right to privacy and data protection is guaranteed by Article 8 of the European Convention on Human Rights, which guarantees the right to respect privacy in all spheres of life, including personal and family life. Personal

* PhD student at the Géza Marton Doctoral School of Legal Studies, University of Debrecen.

¹ A. Michael FROOMKIN: *The Death of Privacy?* *Stanford Law Review*, Vol. 52. 1999. 1463. <http://personal.law.miami.edu/pdf> [Accessed on January 9, 2023].

² Ibid. 1463–1465.

³ Neil M. RICHARDS: *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford University Press, 2014. / 5. <<https://law.duke.edu/sites/pdf>>, [Accessed on January 9, 2023].

data protection is also ensured by the EU's founding treaty, the Treaty on the Functioning of the European Union.

The fundamental rights to data protection and privacy are recognized as separate basic rights under EU law in articles seven and eight of the EU Charter of Fundamental Rights (hereinafter 'EU Charter').⁴ The General Data Protection Regulation,⁵ which replaced the Data Protection Directive 95/46/EC (hereafter 'Data Protection Directive'),⁶ is quite important nowadays due to its establishment of a common standard for personal data protection across the whole European Union. The GDPR and the EU Cookie Policy combine to form the strongest personal data protection framework in the world, requiring end users⁷ to provide a traditional type of consent before enabling cookies to be activated on their websites.

The 97/66/EC Directive (Privacy and Personal Data in Telecommunications), which was repealed by the E-Privacy Directive on July 31, 2002, dealt with the processing of personal data and the security of privacy in the telecommunications market, particularly digital networks in inclusive services and digital mobile networks in public.⁸ A *lex specialis* statute called the E-Privacy Directive adds to the GDPR⁹ by establishing a particular legal framework for privacy and telecommunications. However, the E-Privacy Directive will be repealed when the new E-Privacy Regulation takes effect.¹⁰

⁴ European Union: Council of the European Union, Charter of Fundamental Rights of the European Union. C 303/1. 2007. <<https://www.refworld.org/docid/50ed4f582.html>>, [Accessed on January 9, 2023].

⁵ European Union: Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing 95/46/EC Directive (General Data Protection Regulation). hereafter 'GDPR.' 2016. <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>, [Accessed on January 9, 2023].

⁶ Article 94 of the GDPR, hereafter 'Art.'

⁷ Art. 2(14) of the Directive (EU) 2018/172 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code, L 321/36. Official Journal of the European Union. 2018. <<https://eur-lex.europa.eu/>>, [Accessed on January 9, 2023].

⁸ Heather ROWE: Telecoms Data Protection – UK Implementation. *Computer Law & Security Report*, Vol. 14. No. 6. 1998. 407. <<https://reader.elsevier.com/reader/>>, [Accessed on January 9, 2023].

⁹ Article 29 Data Protection Working Party: Opinion 15/2011 on the Definition of Consent. hereafter '29WP, Opinion 15/2011 on the Definition of Consent.' 11/EN. WP187. 2011. 28. <<https://ec.europa.eu/justice/>>, [Accessed on January 9, 2023].

¹⁰ European Commission: Proposal for an ePrivacy Regulation. Policies. 2022. <<https://digital-strategy.ec/>>, [Accessed on January 9, 2023].

Therefore, the European Union stands out at first appearance for having rather strict laws governing the protection of personal data. However, it is fascinating to see how well strict laws safeguard users' personal data when dealing with cookie regulations. It is obvious that nowadays, users frequently meet infringement from website owners, casting doubt on the legality of employing website cookies. Specifically, dark patterns, a technique for deceiving a user into providing more permission than necessary, could be applied to cookie notices to deceive the user into providing more consent than necessary with the help of, for example, object size, text, and button color. Hence, in this paper, we are going to outline the problems of generally passive consent through the case of Planet 49.

2. The Framework of the Study

2.1. Theoretical Context

Since 2009, the EU Commission has made it essential for websites to obtain informed consent from users accessing from the EU region before installing cookies in their devices in order to address the privacy concerns directly related to cookies. To obtain cookie consent, the majority of websites have been using cookie banners or pop-up windows. According to a 2019 study that examined over 35000 websites, 49% of websites do not adhere to the EU directive, or the 'cookie law,' as it is sometimes known. 74% of websites set third-party cookies without getting the user's permission.¹¹ And a certain number of websites use passive consent from users, which at first glance creates the impression of compliance with regulations, but in fact, violates personal data protection rules. And the case discussed by us also refers to the mentioned case.

Specifically, on the German Federal Supreme Court's request for a preliminary finding in Case C-673/17 (Planet49),¹² the European Court of Justice rendered a decision in late 2019. The questions originating from the underlying dispute between Planet49 GmbH, an online gaming company, and the Federal Union

¹¹ Martino TREVISAN – Stefano TRAVERSO – Eleonora BASSI – Marco MELLIA: *4 Years of EU Cookie Law: Results and Lessons Learned*. Sciendo, 2019. 126–145. Download from: <<https://www.researchgate.net>>, [Accessed on January 9, 2023].

¹² European Court of Justice: Case C-673/17. *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. (hereafter 'Planet49') 2019. 58. <<https://curia.europa.eu/juris/liste.jsf?num=C-673/17>>, [Accessed on January 9, 2023].

of Consumer Organizations and Associations concern consenting to data processing in online contexts and related problems. Specifically, the European Court of Justice held in the case Planet49 that the main focus should be on obtaining active consent from the user, and passive and pre-ticked boxes are not in compliance with EU personal data protection law. The Court also offered direction regarding the scope of the current informative obligations in this aspect. Furthermore, it was determined that whether or not information stored or accessed on a user's terminal device is considered personal data does not matter in terms of Art. 5(3) of the e-Privacy Directive. The bulk of these conclusions are expected and consistent with the principles guiding current data protection and privacy laws. Hence, our research will be devoted to the analysis of the fact that why it is important to ask users for active consent rather than passive consent.

2.2. Legal Context

To get as much knowledge about the subject as possible, we will employ historical, document analysis, and case study methodologies during our study. Through research, the historical method will give us the possibility to thoroughly explore a historical perspective on European telecoms regulation and gain a clear appreciation of the key regulatory trends and the review of the EU regulatory framework for cookie consent. By document analysis method we will mainly focus on the texts of law and articles in order to acknowledge the values and assumptions of the law. And the case study method will allow us to assess the legislative space from a practical point of view.

2.3. Social Context

Social impact is directly and unconditionally related to our protection of personal data. As we know, when a person's personal data is protected, he/she is somewhat insured and safe from potential Internet crimes. And when the purpose of data protection law is to safeguard individuals from the unauthorized gathering of data, storing, and processing – even any nuance that threatens the protection of the personal data of the users requires special attention. Specifically, it requires special attention when it comes to the sharing of our information on the websites through the cookies policies with our consent. However, consent as such needs

to be observed, since if the consent is passive, it cannot be compliant with the law of personal data protection just because it has the name of consent.

3. Data and Information

3.1. Context and Characteristics Cookies

For a better analysis of the cookies, it is necessary to study their context and types. Simply Cookies or HTTP Cookies are clever small text files that are sent by websites to their user's devices for behavior-storing purposes.¹³ These pieces of information enable online service providers to recognize the user's device during subsequent visits to the website.¹⁴ After that, cookies will stay on the user's device for a predetermined amount of time to collect data about the user in order to further the website's varied goals.¹⁵ A cookie can be used as a special identifier that connects the data subject's activity to the device¹⁶ and can gather information regarding the pages that the user has visited, the user identification number, already viewed adverts, and any other information related to the user that the website wants to know.¹⁷ Hence, cookies allow websites to personal user information, enabling them to track users' behaviors and interests.

In other words, most websites keep a little amount of information known as cookies in users' browsers while they are exploring the internet. These cookies are utilized by the website for crucial functions like session management, but they can also be used for consumer tracking or the personalization of advertisements. While websites aim to improve the experience of users by cookies are not intrusive, the collecting and using of such information with the

¹³ Article 29 Data Protection Working Party: Working Document: Privacy on the Internet – An Integrated EU Approach to On-line Data Protection. (Hereafter: Working Document: 'Privacy on the Internet') 2000. 16. <<https://ec.europa.eu>>, [Accessed on January 9, 2023]. see also, Frederic DEBUSSERE: The EU Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster? *International Journal of Law and Information Technology*, Vol. 13, No. 1, 2005. 76. <<https://www.law.kuleuven.be>>, [Accessed on January 9, 2023].

¹⁴ Information Commissioner's Office: Guidance on the rules of Use of Cookies and Similar Technologies. Privacy and Electronic Communications Regulations. 2012. / 2. <<https://ico.org.uk>>, [Accessed on January 9, 2023].

¹⁵ Working Document: Privacy on the Internet op. cit. 16.

¹⁶ Christina MARKOU: Behavioural Advertising and the New 'EU Cookie Law' as a Victim of Business Resistance and a Lack of Official Determination. In: Serge GUTWIRTH – Ronald LEENES – Paul DE HERT (eds.): *Data Protection on the Move*. Vol. 24. 2015. 215.

¹⁷ Ibid.

aim besides those, directly relates to the invasion of privacy.¹⁸ Thus, Cookies may be helpful in some situations for offering a particular service online or for facilitating an internet user's browsing. For instance, some websites rely on cookies to recognize visitors each time they visit, allowing users to check their news without having to log in every time.¹⁹ As a result, some cookies stand out for reasons that are more practical, such as ensuring the web works properly or assisting with its services.

Cookies, which normally have fewer than four kilobytes of memory,²⁰ are utilized in sophisticated advertising tools and serves as the foundation for collecting data on consumers' online browsing habits.²¹ The remarkable era of small text files has started since 1994, thanks to the invention of cookies by Lou Montulli, a ninth Netscape employee. Montulli chose the name 'cookie' for his invention as a nod to an earlier era of computing when systems traded data in what programmers called 'magic cookies.'²² It is worth mentioning that the magic cookies allowed the web owner to know whether the user had returned or not on the website for future use.²³ As a result, it saved users' time and ensured the capabilities of executing online transactions much easier. However, since they might contain a unique identifier that is stored on the user's device and recognizes the data subject when they visit the website again, these clever text files might be regarded as intrusive. Therefore, cookies enable website administrators to carry out covert tracking of a data subject's personal information without that person's knowledge.²⁴

When referring to various cookie kinds, we would like to point out that some cookies can be distinguished by their nature.²⁵ A cookie known as a session cookie or temporary cookie is erased right away as the user closes the browser. Persistent cookies stay on the user's browser until they expire, which may be

¹⁸ Antón ANNIE I. – Qingfeng HE – David L. BAUMER: Inside JetBlue's Privacy Policy Violations. *IEEE Security & Privacy*, 2004. 12–18. In: Anthony D. MIYAZAKI: Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. *Journal of Public Policy & Marketing*, 2008. 21.

¹⁹ Ibid.

²⁰ DEBUSSERE op. cit. 74.

²¹ Thomas BEAUVISAJE – Kevin MELLET: Mobile Consumers and the Retail Industry: The Resistible Advent of a New Marketing Scene. *Researchgate*, 2019. 3.

²² Shane GREENSTEIN: *How the Internet Became Commercial*. Princeton University Press. 2015. 372.

²³ Ibid.

²⁴ Working Document: Privacy on the Internet op. cit. 21.

²⁵ Working Document: Privacy on the Internet op. cit. 42.

minutes, weeks, or even years in some cases.²⁶ Cookies can also be divided into first-party and third-party categories depending on the domain or sender.²⁷ First-party cookies are those that are set by the home page, or, to put it another way, those that are sent and viewed by a company on its website.²⁸ Third parties, typically a network of advertising agencies, that have agreements with various websites for the purpose of displaying advertisements on those websites, set third-party cookies.²⁹

Four sorts of purposes for cookies can be presented: strictly necessary, performance, functionality, and targeted or advertising cookies.³⁰ First off, it should be noted that cookies that are strictly necessary do not require permission due to the fact that these kinds of cookies are necessary for users to navigate websites steadily and access services like secure areas.³¹ While performance cookies improve users' experience online, functionality cookies allow the website to remember user preferences, such as language, location, or other personal information, and deliver better, more individualized services. For instance, a website can provide local weather information by keeping the cookie of the area the user is currently in.³² Cookies that are used for targeting or advertising are intended to provide more ads that are relevant to users' interests. These cookie types monitor the effectiveness of marketing campaigns.³³

3.2. Case Planet 49

Planet49 launched a marketing lottery on the website www.dein-macbook.de, requiring visitors who wished to enter the contest to enter their zip codes, which

²⁶ Article 29 Data Protection Working Party: Opinion 04/2012 on Cookie Consent Exemption. *WP* 194. 2012. 4. <<https://ec.europa.eu/>>, [Accessed on January 9, 2023].

²⁷ Planet49: Opinion of Advocate General Szpunar, *op. cit.* 40.

²⁸ MARKOU *op. cit.* 216.

²⁹ *Ibid.*

³⁰ Cybot A/S: WordPress and GDPR, and How to Deal with Cookies and Plugins. 2019. In: Dominique MACHULETZ – Rainer BÖHME (eds.): *Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR*. 2020. 482. <<https://www.cookiebot.com/>>, [Accessed on January 9, 2023].

³¹ *Ibid.* see also, International Chamber of Commerce: ICC UK Cookie Guide. 2012. 8. <<https://www.cookieclaw.pdf>>, [Accessed on January 9, 2023].

³² *Ibid.*, 9.

³³ *Ibid.*

led them to a page with two boxes.³⁴ The first was a checkbox for receiving adverts from third parties that weren't checked. The second was a pre-ticked box that authorized Planet49 to track the user's online behavior and set cookies. To be eligible to enter the lottery, users had to check at least the first box.³⁵ More precisely, users had to submit their names and addresses in order to participate in the lottery. The page contained two explanations and a button that roughly said, 'Click here to participate free of charge,' along with three other items that were essential to the legal analysis. There was no checkmark in the first checkbox. The accompanying text effectively allowed third parties to get in touch with users via phone, mail, email, etc. for advertising purposes. The next checkbox had a pre-selected checkmark on it. The accompanying paragraph read as follows: 'I agree to the web analytics service Remintrex being used for me. This has the consequence that, following registration for the lottery, the lottery organizer, [Planet49], sets cookies, which enables Planet49 to evaluate my surfing and use behavior on websites of advertising partners and thus enables advertising by Remintrex that is based on my interests. I can delete the cookies at any time. You can read more about this here.'³⁶ So that extensive cookie-based user tracking for advertising purposes was allowed, the second pre-checked box was selected. Before clicking the button, users had to actively check the first checkbox; however, they can also leave the second checkbox unchecked. By unticking the box, users have the choice to decline the offer of cookies. These two check-boxes did not adhere to German law, according to the German Federation of Consumer Organizations, and Planet49 was instructed to stop using them.³⁷ A preliminary ruling was requested from the European Court of Justice after the case eventually made it to the German Federal Court of Justice.³⁸

The Court started by looking at the E-Privacy Directive, which demands explicit consent for data storage. The e-Privacy Directive does not, however, specify how consent must be given. The user must explicitly state their preferences, according to the Court's literal interpretation of the phrase 'given his or her consent.' To put it another way, the CJEU determined that the phrase

³⁴ Planet49 op. cit. 25., 26.

³⁵ Planet49 op. cit. 26., 27., 28.

³⁶ Planet49 op. cit. 27.

³⁷ Planet49 op. cit. 32., 33.

³⁸ Planet49 op. cit. 37.

‘given his or her agreement’ to the usage of cookies requires user behavior.³⁹ This opinion is supported by the requirement that the user express their preferences in both the Data Protection Directive and the GDPR’s definitions of consent, which, according to the court, clearly shows an active activity rather than a passive behavior.⁴⁰ Because of this, consent must be clear-cut, which can only be done by taking action.⁴¹ Simply saying, an action must be active rather than passive. Consequently, the court determined that a pre-selected box did not satisfy the conditions for valid consent.

The CJEU argued that it would be difficult to discern logically whether a user had given agreement to the processing of their data by failing to uncheck a pre-selected box or if such consent had in fact been informed. Additionally, there is a great likelihood that the user won’t read the content that goes along with the pre-ticked checkbox or simply fail to see it.⁴² By not deselecting the pre-ticked box, it is difficult to determine if the user has granted informed consent to the use of his or her data.

In conclusion, active conduct on the part of the user is required for clear consent. Currently, the General Data Protection Regulation does not regard silence, checked boxes, or inaction to be active consent. In other words, methods of getting implicit consent, such as web browsers that accept cookies by default, are no longer permitted. Therefore, website owners should check their cookie rules to ensure that consent that complies with GDPR is obtained.

4. Discussion

Consent is recognized as a legal ground that makes data processing permissible. Despite the fact that there is debate over whether permission is the best strategy for protecting online users’ privacy and personal information, for instance, it’s pretty exhausting for active internet users to respond to tons of cookie banners on the website every day,⁴³ still by giving to the users’ active consent possibility is the best way nowadays to protect their online behavior.

³⁹ Planet49 op. cit. 49.

⁴⁰ Planet49 op. cit. 52.

⁴¹ Planet49 op. cit. 54.

⁴² Planet49 op. cit. 55.

⁴³ Article 29 Working Party: Guidelines 05/2020 on Consent under Regulation 2016/679. Version 1.1. 2020. 17. <<https://edpb.europa.eu>>, [Accessed on January 9, 2023].

The CJEU examined the particular authorization in the context of Planet 49 and ruled that the user's desires had to be precise in the sense that they had to be related solely to the data processing in question and couldn't be inferred from the data subject's wishes for other reasons. As a result, it was incorrect to assume that the user had consented to the storing of cookie files by simply clicking a button to participate in a promotional lottery organized by Planet 49. A similar line of reasoning was adopted by Advocate General Szpunar, who claimed that in order to be 'freely provided and informed,' active consent had to be both distinct and active.⁴⁴ Accordingly, the standard of willingly given and informed permission includes separate permission that is apart from other activities in addition to active activity.

General Szpunar stated that the act of consenting cannot be linked with a user's online behavior, such as accessing a website, watching a movie, participating in a lottery, etc. The granting of consent cannot appear to be secondary in nature in relation to playing the lottery, especially from the perspective of users. Additionally, both activities must be presented equally, particularly visually. Respectively, according to the CJEU's ruling and General Szpunar's opinion, consent cannot be confused with an action that simultaneously suggests another intention or goal. As a result, the focus should be on the distinction between consent and behaviors that suggest other objectives and intentions, and acquiring ancillary consent should be prohibited. To conclude, obtaining active consent is one of the most important conditions for the security of the personal data protection of users.

5. Conclusion

In the modern internet era, data protection has emerged as a key issue. However, given the rapid advancement of technology in the online environment, lawmakers have had difficulty securing personal information. Website owners frequently utilize 'cookies' to enable the capture and processing of enormous amounts of users' personal data. In accordance with Article 5(3) of Directive 2002/58/EC, the user's consent is required for the usage of cookies. However, it is still debatable whether cookie consent policies actually safeguard internet

⁴⁴ European Court of Justice: Case C-673/17. *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* OJ C 413. Opinion of Advocate General Szpunar. 2019.

users and provide them control over how their data collected through cookies is used.

In exchange for their personal information, users of the internet can connect and access a wealth of free resources and services. Numerous websites utilize cookie technology to gather data about their users and visitors. Cookies can be used for a variety of things, including keeping track of user preferences, monitoring online activity, creating user profiles, and delivering targeted advertising based on those profiles. Thus, they might violate someone's privacy.

After considering the aforementioned, we can state that due to the rapid expansion of the virtual world, more severe and effective measures are required to maximize the protection of one of the most valuable resources – data or information.⁴⁵

⁴⁵ The World's Most Valuable Resource Is No Longer Oil, but Data. Leaders/Regulating the Internet Giants. *The Economist*, 2017. <<https://www.economist.com>>, [Accessed on January 9, 2023].