Cookies, privacy and data protection

Cookies, privacidade e proteção de dados

10.29073/j2.v8i1.1124

Recebido: 01 de fevereiro de 2026.
Aprovado: 25 de março de 2026.
Publicado: 04 de abril de 2026.

Autor/a: Sílvia Cardoso, ESTG-IPP, Portugal, silviacardosolg@gmail.com.

Abstract

This paper aims to analyze issues related to cookies, privacy, and data protection, providing a critical overview of relevant literature and regulatory frameworks. It examines the implications of cookie usage in the context of the General Data Protection Regulation (GDPR), highlights current challenges, and discusses emerging trends such as the decline of third-party cookies and the rise of alternative tracking technologies. The paper concludes by proposing measures that organizations should adopt to ensure compliance and enhance user privacy in an evolving digital landscape.

Keywords: Cookies; Data Protection; ePrivacy; GDPR; Privacy.

Resumo

Este artigo tem como objetivo analisar questões relacionadas a cookies, privacidade e proteção de dados, fornecendo uma visão crítica da literatura relevante e dos marcos regulatórios. Examina as implicações do uso de cookies no contexto do Regulamento Geral de Proteção de Dados (RGPD), destaca os desafios atuais e discute tendências emergentes, como o declínio dos cookies de terceiros e a ascensão de tecnologias alternativas de rastreamento. O artigo conclui propondo medidas que as organizações devem adotar para garantir a conformidade e aprimorar a privacidade do usuário em um cenário digital em constante evolução.

Palavras-Chave: Cookies; Privacidade; Privacidade Eletrónica; Proteção de Dados; RGPD.

1. Introduction

Cookies, defined as small text files stored in a user's web browser when visiting a website, are a fundamental component of modern web technologies. They serve multiple purposes, including session management, personalization, and targeted advertising. However, due to their ability to collect and store significant amounts of user data, cookies raise substantial concerns regarding privacy and data protection.

With the enforcement of the General Data Protection Regulation (GDPR), stricter requirements were introduced regarding the processing of personal data, including data derived from cookies. The GDPR emphasizes transparency, accountability, and the need for explicit user consent(European Union, 2016). However, despite these requirements, many websites continue to implement inadequate consent mechanisms. As a result, the existing ePrivacy framework has been increasingly scrutinized, revealing regulatory gaps and the need for further legal harmonization.

In recent years, additional developments – such as stricter enforcement by data protection authorities and technological changes in tracking mechanisms – have significantly reshaped the landscape of online privacy. Notably, the progressive elimination of third-party cookies by major web browsers and the emergence of alternative tracking technologies have introduced new challenges and regulatory considerations.

Recent enforcement actions by European data protection authorities have reinforced the importance of valid consent, particularly in relation to misleading cookie banners and the use of manipulative design practices (CNIL,

2024). These developments highlight the need for continuous adaptation of both legal frameworks and organizational practices.

Furthermore, the rapid evolution of digital technologies and business models has made data protection an increasingly complex and dynamic field, requiring continuous adaptation of both legal and technical approaches.

2. Related Work

Several studies have explored the relationship between cookies and data protection, highlighting both legal and practical implications.

The study by Lima et al. (2023) compares cookie policies under the Brazilian LGPD and the European GDPR. It concludes that user consent mechanisms are often ineffective, as users are frequently compelled to accept terms to access online services. Furthermore, it emphasizes that the GDPR provides a more detailed and restrictive framework than other regulations.

Jayakumar (2021) investigates user attitudes toward cookie consent banners in the European Union. It highlights that factors such as design, trust, and perceived risk significantly influence user behavior. Importantly, it anticipates the decline of third-party cookies and suggests the emergence of more complex tracking technologies, reinforcing the need for enhanced regulatory frameworks.

Another study by Alharbi et al. (2023), evaluates compliance and usability of cookie interfaces. The findings reveal widespread use of manipulative design practices (dark patterns), with many websites failing to provide adequate privacy information or meaningful consent options.

Similarly, Cui (2021) presents empirical evidence showing that, despite regulatory requirements, many websites still fail to provide effective user control. Even when users attempt to reject cookies, tracking mechanisms often persist.

More recent studies reinforce these findings. Nouwens et al. (2025) highlight that a significant number of websites remain non-compliant with GDPR requirements, particularly due to the absence of clear rejection options. Additionally, Grossman et al. (2025) demonstrate that many cookie banners use manipulative design techniques to influence user behavior, undermining the validity of consent.

3. Challenges and Opportunities

3.1. Challenges

The use of cookies and similar tracking technologies raises several critical challenges.

Cookies enable extensive tracking and profiling of users across multiple websites, allowing organizations to build detailed behavioral profiles. This practice raises serious privacy concerns and may constitute an intrusion into user's personal lives.

Furthermore, cookies facilitate the collection and storage of large volumes of personal data, increasing the risk of unauthorized access and data breaches. The lack of transparency regarding how data is collected and used further exacerbates these concerns.

The protection of informational self-determination remains a critical challenge in the context of online tracking. Despite regulatory requirements, users often lack effective control over their data. Many websites implement interfaces that make it difficult to refuse cookies, frequently using manipulative design strategies known as dark patterns (CNIL, 2024; Grossman et al., 2025). These manipulative practices not only undermine user autonomy but also call into question the validity of consent under the GDPR framework (CNIL, 2024).

In addition, recent research indicates that tracking may persist even when users explicitly reject cookies, raising concerns about the effectiveness of consent mechanisms (Rasaii et al., 2025).

The ongoing evolution of tracking technologies also presents new regulatory challenges. As third-party cookies are progressively phased out, alternative techniques such as browser fingerprinting are becoming more prevalent, often operating outside traditional regulatory frameworks.

3.2. Opportunities

Despite these challenges, cookies and related technologies also present several benefits.

They enable personalized user experiences, improving usability and efficiency. Additionally, cookies support targeted advertising, allowing organizations to deliver more relevant content to users.

Cookies also play an important role in enhancing security, particularly in authentication processes and fraud detection. Moreover, the development of privacy-enhancing technologies, such as virtual private networks (VPNs) and ad blockers, provides users with greater control over their data.

Finally, evolving regulatory frameworks encourage organizations to adopt more transparent and user-centric data practices, contributing to improved privacy protection.

4. Recent Developments (Update)

In recent years, significant changes have reshaped the digital privacy landscape.

Data protection authorities have intensified enforcement actions, imposing substantial fines for non-compliance with cookie regulations (CNIL, 2025, 2026). These actions demonstrate a growing commitment to ensuring that organizations adhere to GDPR requirements. In practice, many widely used websites still implement non-compliant cookie banners, demonstrating a persistent gap between legal requirements and real-world implementation.

At the same time, major technology companies have begun phasing out third-party cookies, marking a significant shift in online tracking and advertising practices. This transition is leading to the emergence of alternative tracking technologies, which poses significant challenges for privacy protection.

In addition to the GDPR, the European Union has been working on the proposed ePrivacy Regulation, which is intended to replace the current ePrivacy Directive and provide more specific rules regarding electronic communications and the use of tracking technologies such as cookies.

The ePrivacy Regulation aims to strengthen user confidentiality, regulate the use of metadata, and ensure stricter conditions for storing and accessing information on user devices. In particular, it reinforces the requirement for prior user consent for non-essential cookies and seeks to address emerging tracking techniques that are not fully covered by existing legislation.

However, despite its relevance, the regulation has faced delays and has not yet been fully adopted, creating ongoing legal uncertainty in the field of online privacy (European Union, 2016). This delay highlights the difficulty of regulating rapidly evolving technologies, particularly in the context of digital advertising and data-driven business models.

5. Conclusions

Cookies remain a central component of the modern digital ecosystem, particularly in areas such as marketing and personalization. However, their use continues to raise important concerns regarding privacy and data protection.

While the GDPR has established a strong legal foundation, ongoing technological developments and evolving tracking practices require continuous regulatory adaptation. The increasing use of alternative tracking methods further complicates the landscape, highlighting the need for more robust and comprehensive solutions.

To address these challenges, organizations should adopt several key measures. These include ensuring transparency in data collection practices, limiting the use of third-party cookies, implementing strong security mechanisms, and providing users with clear and accessible control options.

Additionally, organizations must obtain explicit and informed consent, avoid manipulative interface designs, and define clear data retention policies. These measures are essential to ensure compliance with regulatory requirements and to protect users' fundamental rights.

Achieving a balance between technological innovation and privacy protection is crucial. As the digital environment continues to evolve, both legal frameworks and organizational practices must adapt to ensure that user privacy is effectively safeguarded. Ultimately, safeguarding user privacy in the digital age is not only a legal obligation but a fundamental requirement for maintaining trust in modern data-driven ecosystems.

Despite the existence of robust legal frameworks, there is a persistent gap between regulation and practice, as many organizations continue to implement non-compliant tracking mechanisms. This suggests that enforcement alone may not be sufficient, requiring a combination of technological solutions, user awareness, and stricter accountability mechanisms.

References

Alharbi, J. A., Albesher, A. S., & Wahsheh, H. A. (2023). An empirical analysis of e-governments' cookie interfaces in 50 countries. *Sustainability, 15*(2), 1231. https://www.mdpi.com/2071-1050/15/2/1231

Commission Nationale de l'Informatique et des Libertés (CNIL). (2024). *Dark patterns in cookie banners: CNIL issues formal notice to website publishers*. https://www.cnil.fr/en/dark-patterns-cookie-banners-cnil-issues-formal-notice-website-publishers

Commission Nationale de l'Informatique et des Libertés (CNIL). (2025). *Cookie regulation: CNIL continuing action plan and sanctions*. https://www.cnil.fr/en/cookie-regulation-cnil-continuing-action-plan-initiated-2019-and-has-imposed-two-fines-shein-and

Commission Nationale de l'Informatique et des Libertés (CNIL). (2026). *Sanctions and corrective measures: CNIL's actions in 2025*. https://www.cnil.fr/en/sanctions-and-corrective-measures-cnils-actions-2025

Cui, Y. (2021). *Measure cookie setting behavior of web pages showing cookie privacy warnings* (Master's thesis, University of Edinburgh). https://groups.inf.ed.ac.uk/tulips/projects/20-21/cui.pdf

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504

Grossman, R., Smith, M., Borcea, C., & Chen, Y. (2025). Using salient object detection to identify manipulative cookie banners that circumvent GDPR. https://arxiv.org/pdf/2510.26967

Jayakumar, L. N. (2021). Cookies 'n' consent: An empirical study on the factors influencing website users' attitudes towards cookie consent in the EU. *DBS Business Review*. https://dbsbusinessreview.ie/index.php/journal/article/view/72

Lima, C. R. C., Silva, I. F. S., Silva, R. D., & Carr, C. N. (2023). Cookies and their close relationship with data protection policy. *Brazilian Journal of Development*. https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/56231/41313

Nouwens, M., Kristensen, J. B., Maalt, K., & Bagge, R. (2025). A cross-country analysis of GDPR cookie banners and compliance: Flexible methods for scraping them.

Rasaii, A., Dao, H., Feldmann, A., Javid, M., Gasser, O., & Gosain, D. (2025). Intractable cookie crumbs: Unveiling the nexus of stateful banner interaction and tracking cookies. https://www.researchgate.net/publication/395442240_Intractable_Cookie_Crumbs_Unveiling_the_Nexus_of_Stateful_Banner_Interaction_and_Tracking_Cookies

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.

Todo o conteúdo do ***J² — Jornal Jurídico*** é licenciado sob Creative Commons, a menos que especificado de outra forma e em conteúdo recuperado de outras fontes bibliográficas.